53-1001931-01
Sept 2010

Brocade Mobility RFS4000, RFS6000 and RFS7000

CLI Reference Guide

Supporting software release 4.3.0.0 and later

BROCADE

Brocade Communications Systems, Incorporated

Corporate and Latin American Headquarters
Brocade Communications Systems, Inc.
130 Holger Way
San Jose, CA 95134
Tel: 1-408-333-8000
Fax: 1-408-333-8101
E-mail: info@brocade.com

Asia-Pacific Headquarters
Brocade Communications Systems China HK, Ltd.
No. 1 Guanghua Road
Chao Yang District
Units 2718 and 2818
Beijing 100020, China
Tel: +8610 6588 8888
Fax: +8610 6588 9999
E-mail: china-info@brocade.com

European Headquarters
Brocade Communications Switzerland Sàrl
Centre Swissair
Tour B - 4ème étage
29, Route de l'Aéroport
Case Postale 105
CH-1215 Genève 15
Switzerland
Tel: +41 22 799 5640
Fax: +41 22 799 5641
E-mail: emea-info@brocade.com

Asia-Pacific Headquarters
Brocade Communications Systems Co., Ltd. (Shenzhen WFOE)
Citic Plaza
No. 233 Tian He Road North
Unit 1308 – 13th Floor
Guangzhou, China
Tel: +8620 3891 2000
Fax: +8620 3891 2111
E-mail: china-info@brocade.com

Document History

Title	Publication number	Summary of changes	Date
Brocade Mobility RFS4000, RFS6000 and RFS7000 CLI Reference Guide	*53-1001931-01*	Additions for software version 4.3.0.0	Sept 2010

About This Document

In this chapter

Audience

This document is designed for system administrators with a working knowledge of Layer 2 and Layer 3 switching and routing.

If you are using a Brocade Layer 3 router, you should be familiar with the following protocols if applicable to your network – IP, RIP, OSPF, BGP, ISIS, IGMP, PIM, DVMRP, and VRRP.

To avoid confusion among Mobility RFS4000 Controller, Mobility RFS6000 Controller and Mobility RFS7000 Controller CLI users, generic examples are used throughout this guide. These examples are relevant to each controller.

Example

```
RFController>cluster-cli enable
RFController>
```

The syntax, parameters and descriptions within this guide can also be used generically for a Mobility RFS4000 Controller, Mobility RFS6000 Controller and Mobility RFS7000 Controller. However, some subtle differences do exist amongst these baselines. These differences are strongly noted within the specific commands impacted. When these differences are noted, the options available to each controller baseline are described in detail.

How to use this guide

This guide will help you implement, configure, and administer the controller and associated network elements. This guide is organized into the following sections:

Chapter	Jump to this section if you want to...
Chapter 1, "Introduction"	Review the overall feature-set of the controller, as well as the many configuration options available.
Chapter 2, "Common Commands"	Understand the commands common amongst many contexts and instance contexts within the controller CLI.
Chapter 3, "User Exec Commands"	Summarize the User Exec commands within the controller CLI.
Chapter 4, "Privileged Exec Commands"	Review the Priv Exec commands within the controller CLI.
Chapter 5, "Global Configuration Commands"	Understand the Global Config commands within the controller CLI.
Chapter 6, "Crypto-isakmp Instance"	Review the **(crypto-isakmp)** commands within the controller CLI.
Chapter 7, "Crypto-group Instance"	Understand the **(crypto-group)** commands within the controller CLI.
Chapter 8, "Crypto-peer Instance"	Summarize the **(crypto-peer)** commands within the controller CLI.
Chapter 9, "Crypto-ipsec Instance"	Review the **(crypto-ipsec)** commands within the controller CLI.
Chapter 10, "Crypto-map Instance"	Understand the **(crypto-map)** commands within the controller CLI.
Chapter 11, "Crypto-trustpoint Instance"	Summarize the **(crypto trustpoint)** commands within the controller CLI.
Chapter 12, "Interface Instance"	Understand the **(config-if)** commands within the controller CLI.
Chapter 13, "Spanning tree-mst Instance"	Summarize the **(config-mst)** instance commands within the controller CLI.
Chapter 14, "Extended ACL Instance"	Review the **(config-ext-nacl)** commands within the controller CLI.
Chapter 15, "Standard ACL Instance"	Understand the **(config-std-nacl**) commands within the controller CLI.
Chapter 16, "Extended MAC ACL Instance"	Review the **(config-ext-macl)** commands within the controller command line.
Chapter 17, "DHCP Server Instance"	Understand the **(config-dhcp-pool)** commands within the controller command line.
Chapter 18, "DHCP Class Instance"	Review the **(config-dhcp-class)** instance commands within the controller CLI.
Chapter 19, "Radius Server Instance"	Summarize the **(config-radsrv)** instance commands within the controller CLI.
Chapter 20, "Wireless Instance"	Understand the **(config-wireless)** instance commands within the controller CLI.
Chapter 21, "RTLS Instance"	Review the **(config-rtls)** instance commands within the controller CLI.

Chapter	Jump to this section if you want to...
Chapter 22, "ESPI Instance"	Review the **(config-rtls-espi)** instance commands within the controller CLI
Chapter 23, "RFID Instance"	Review the **(config-rtls-rfid)** instance commands within the controller CLI
Chapter 24, "SOLE Instance"	Review the **(config-rtls-sole)** instance commands within the controller CLI
Chapter 25, "Smart RF Instance"	Review the **(config-wireless-smart-rf)** instance commands within the controller CLI
Chapter 26, "Role Instance"	Review the **(config-role)** instance commands within the controller CLI

Supported hardware and software

The following hardware platforms are supported by this release of this guide:

- Brocade Mobility RFS7000 Controller
- Brocade Mobility RFS6000 Controller
- Brocade Mobility RFS4000 Controller

The following software versions are supported by this release of this guide:

- Software version 4.3.0.0 and later

Document conventions

This section describes text formatting conventions and important notice formats used in this document.

Text formatting

The narrative-text formatting conventions that are used are as follows:

bold text	Identifies command names
	Identifies the names of user-manipulated GUI elements
	Identifies keywords
	Identifies text to enter at the GUI or CLI
italic text	Provides emphasis
	Identifies variables
	Identifies document titles
`code` text	Identifies CLI output

For readability, command names in the narrative portions of this guide are presented in mixed lettercase: for example, controllerShow. In actual examples, command lettercase is often all lowercase. Otherwise, this manual specifically notes those cases in which a command is case sensitive.

Command syntax conventions

command / keyword	The first word is always a command. Keywords are words that must be entered as is. Commands and keywords are mandatory.
	For example, the command,
	`RFController>show wlan 1`
	is documented as
	`show wlan <idx>`
	where:
	• show – The command
	• wlan – The keyword

<variable>	Variables are described with a short description enclosed within a '<' and a '>' pair.
	For example, the command,
	`RFController>show wlan 1`
	is documented as
	`show wlan <idx>`
	where:
	• show – The command – Display information.
	• wlan – The keyword – The wlan
	• <idx> – The variable – WLAN Index value.

|	The pipe symbol. This is used to separate the variables/keywords in a list.
	For example, the command
	`RFController> show .....`
	is documented as
	`show [autoinstall|banner|ip|ldap|......]`
	where:
	• set – The command
	• [autoinstall|banner|ip|ldap|.....] – Indicates the different commands that can be combined with the show command. However, only one of the above list can be used at a time.
	`show autoinstall ...`
	`show banner ...`
	`show ip ...`
	`show ldap ...`

[ ]	Of the different keywords and variables listed inside a '[' & ']' pair, only one can be used. Each choice in the list is separated with a '|' (pipe) symbol.
	For example, the command
	`RFController> clear ...`
	is documented as
	`clear [crypto|mobility|spanning-tree]`
	where:
	• clear – The command
	• [crypto|mobility|spanning-tree] – Indicates that three keywords are available for this command and only one can be used at a time

{ }	Any command/keyword/variable or a combination of them inside a '*{*' & '*}*' pair is optional. All optional commands follow the same conventions as listed above. However they are displayed italicized.
	For example, the command
	`RFController> show autoinstall ....`
	is documented as
	`show autoinstall {status}`
	Here:
	• show autostatus– The command. This command can also be used as
	`show autostatus`
	• *{status}* – The optional keyword status. The command can also be extended as
	`show autoinstall status`
	Here the keyword *status* is optional.

<values>	Values to be entered as shown in Blue.
	For example, the command
	`RFController>show wlan 1`
	is documented as
	`show wlan <idx>`
	This command's parameter <idx> is described as under:
	"<idx> – <idx> (1-256) is the Wlan Index."

Notes, cautions, and warnings

The following notices and statements are used in this manual. They are listed below in order of increasing severity of potential hazards.

NOTE
A note provides a tip, guidance or advice, emphasizes important information, or provides a reference to related information.

CAUTION

A Caution statement alerts you to situations that can be potentially hazardous to you or cause damage to hardware, firmware, software, or data.

DANGER

A Danger statement indicates conditions or situations that can be potentially lethal or extremely hazardous to you. Safety labels are also attached directly to products to warn of these conditions or situations.

Notice to the reader

This document may contain references to the trademarks of the following corporations. These trademarks are the properties of their respective companies and corporations.

These references are made for informational purposes only.

Corporation	Referenced trademarks and products
Phillips Screw Company, Inc.	Phillips

Web support sites

Product downloads

http://www.brocade.com

Manuals

http://www.brocade.com

Additional information

http://www.brocade.com

Chapter

Introduction 1

In this chapter

This chapter describes the commands defined by the controller *Command Line Interface* (CLI). Access the CLI (on the supported Mobility RFS6000 Controller and Mobility RFS7000 Controller models) by running a terminal emulation program on a computer connected to the serial port on the front of the controller, or by using a Telnet session via *secure shell* (SSH) to access the controller over the network. The default CLI user designation is *cli*. The default username and password are *admin* and *admin123* respectively.

To avoid confusion amongst Mobility RFS6000 Controller and Mobility RFS7000 Controller CLI users, generic examples are used throughout this guide. These examples are relevant to each controller.

Example

```
RFController>cluster-cli enable
RFController>
```

The CLI syntax, parameters and descriptions within this guide can also be used generically for a Mobility RFS4000 Controller, Mobility RFS6000 Controller and Mobility RFS7000 Controller model. However, some subtle differences do exist amongst these baselines. These differences are noted within the specific commands impacted. When these differences are noted, the options available to each controller baseline are described in detail.

CLI overview

The CLI is used for configuring, monitoring, and maintaining the controller managed network. The user interface allows you to execute commands (on the supported Mobility RFS4000 Controller, Mobility RFS6000 Controller and Mobility RFS7000 Controller models) using either a serial console or a remote access method.

This chapter describes the basic features of the CLI. Topics covered include an introduction to command modes, navigation and editing features, help features, and command history.

Configuration for connecting to the CLI using a terminal emulator

Use the following settings to configure your terminal emulator for connecting to the controller's CLI.

Bits Per Second	19200
Data Bits	8
Parity	None
Stop Bit	1
Flow Control	None

When a CLI session is established, to access the controller, do as follows (user input is in bold)

```
login as: cli

User Access Verification

Username:
```

Use the following credentials when logging to the CLI for the first time.

User Name	admin
Password	admin123

When logging for the first time, you are prompted to change the password.

CLI Modes

The CLI is segregated into different command modes. Each mode has its own set of commands for configuration, maintenance and monitoring. The commands available at any given time depend on the mode you are in, and to a lesser extent, the particular Mobility RFS6000 Controller or Mobility RFS7000 Controller model used. Enter a question mark (**?**) at the system prompt to view a list of commands available for each command mode/instance.

Use specific commands to navigate from one command mode to another. The standard order is: USER EXEC mode, PRIV EXEC mode and GLOBAL CONFIG mode.

A session generally begins in the USER EXEC mode (one of the two access levels of the EXEC mode). For security, only a limited subset of EXEC commands are available in the USER EXEC mode. This level is reserved for tasks that do not change the configuration of the controller (such as determining the current controller configuration).

To access commands, enter the PRIV EXEC mode (the second access level for the EXEC mode). Once in the PRIV EXEC mode, enter any EXEC command. The PRIV EXEC mode is a superset of the USER EXEC mode.

Most of the USER EXEC mode commands are one-time commands and are not saved across controller reboots. For example, the show command displays the current configuration and the clear command clears the interface.

Access the GLOBAL CONFIG mode from the PRIV EXEC mode. In GLOBAL CONFIG mode, enter commands that set general system characteristics. Configuration modes, allow you to change the running configuration. If you save the configuration later, these commands are stored across controller reboots.

Access a variety of protocol-specific (or feature-specific) modes from the global configuration mode. The CLI hierarchy requires you access specific configuration modes only through the global configuration mode.

You can also access sub-modes from the global configuration mode. Configuration sub-modes define specific features within the context of a configuration mode.

Table 1 summarizes the commands available from the controller.

TABLE 1 RF Controller CLI Hierarchy

User Exec Mode	Priv Exec Mode	Global Configuration Mode
clear	acknowledge	aaa
clrscr	archive	access-list
cluster-cli	cd	autoinstall
disable	change-passwd	banner
enable	clear	boot
exit	clock	bridge
help	clrscr	clrscr
logout	cluster-cli	country-code
no	configure	crypto
page	copy	do
ping	debug	end
quit	delete	errdisable
service	diff	exit
show	dir	ftp
telnet	disable	help
terminal	edit	hostname
traceroute	enable	interface
	erase	ip
	exit	license
	halt	line
	help	local
	kill	logging
	logout	mac
	mkdir	mac-address-table
	more	mac-name
	no	management
	page	no

TABLE 1 RF Controller CLI Hierarchy

User Exec Mode	Priv Exec Mode	Global Configuration Mode
	ping	ntp
	pwd	prompt
	quit	radius-server
	reload	redundancy
	rename	rtls
	rmdir	service
	service	show
	show	smtp-notification
	telnet	snmp-server
	terminal	spanning-tree
	traceroute	timezone
	upgrade	traffic-shape
	upgrade-abort	username
	write	vpn
	format	wireless
		wireless-acl
		firewall
		network-element-id
		ratelimit
		role
		virtual-ip
		wwan

To return from the Global Config mode to the Privilege Exec mode use:

```
RFSController(config)#exit
RFSController#
```

Similarly, to return from the Privilege Exec mode to User Exec mode use

```
RFSController#disable
RFSController>
```

Getting context sensitive help

Enter a question mark (**?**) at the system prompt to display a list of commands available for each mode. Obtain a list of arguments and keywords for any command using the CLI context-sensitive help.

Use the following commands to obtain help specific to a command mode, command name, keyword or argument:

Command	Description
(prompt)# help	Displays a brief description of the help system
(prompt)# abbreviated-command-entry?	Lists commands in the current mode that begin with a particular character string
(prompt)# abbreviated-command-entry<Tab>	Completes a partial command name
(prompt)# ?	Lists all commands available in the command mode
(prompt)# command ?	Lists the available syntax options (arguments and keywords) for the command
(prompt)# command keyword ?	Lists the next available syntax option for the command

NOTE
The system prompt varies depending on which configuration mode you are in.

NOTE
Enter **Ctrl + V** to use **?** as a regular character and not as a character used for displaying context sensitive help. This is required when the user has to enter a URL that ends with a ?

NOTE
The escape character used through out the CLI is “\”. To enter a "\" use "\\" instead.

When using context-sensitive help, the space (or lack of a space) before the question mark (?) is significant. To obtain a list of commands that begin with a particular sequence, enter the characters followed by a question mark (?). Do not include a space. This form of help is called **word help**, because it completes a word.

```
RFController#service?
  service Service Commands

RFController#service
```

Enter a question mark (?) (in place of a keyword or argument) to list keywords or arguments. Include a space before the **?**. This form of help is called **command syntax help.** It shows the keywords or arguments available based on the command/keyword and argument already entered.

```
RFController>service ?
  diag      Diagnostics
  encrypt   Encrypt password or key with secret
  save-cli  Save CLI tree for all modes in html format
  show      Show running system information

RFController>service
```

It is possible to abbreviate commands and keywords to allow a unique abbreviation. For example, “configure terminal” can be abbreviated as `config t`. Since the abbreviated command is unique, the controller accepts the abbreviation and executes the command.

Enter the help command (available in any command mode) to provide the following description:

```
RFController>help
CLI provides advanced help feature.  When you need help,
```

```
anytime at the command line please press '?'.

If nothing matches, the help list will be empty and you must backup
until entering a '?' shows the available options.
Two styles of help are provided:
1. Full help is available when you are ready to enter a
   command argument (e.g. 'show ?') and describes each possible
   argument.
2. Partial help is provided when an abbreviated argument is entered
   and you want to know what arguments match the input
   (e.g. 'show ve?'.)

RFController>
```

Using the no and default command forms

Almost every command has a `no` form. Use no to disable a feature or function. Use the command without the `no` keyword to re-enable a disabled feature or enable a feature disabled by default.

Basic conventions

Keep the following conventions in mind while working within the CLI:

- Use **?** at the end of a command to display available sub-modes . Type the first few characters of the sub-mode and press the tab key to add the sub-mode. Continue using **?** until you reach the last sub-mode
- Pre-defined CLI commands and keywords are case-insensitive: `cfg = Cfg = CFG`. However (for clarity), CLI commands and keywords are displayed (in this guide) using mixed case. For example, `apPolicy`, `trapHosts`, `channelInfo`
- Enter commands in uppercase, lowercase, or mixed case. Only passwords are case sensitive
- If an instance name (or other parameter) contains whitespace, the name must be enclosed in quotes

```
RFController.(Cfg)> spol "Default Controller Policy"
RFController.(Cfg).SPolicy.[Default Controller Policy]>
```

NOTE
Commands starting with `#` at the `RFController#` prompt are ignored and not executed. Any space before a CLI command is ignored in execution.

Using CLI editing features and shortcuts

A variety of shortcuts and edit features are available. The following describe these features:

- *Moving the cursor on the command line*
- *Completing a partial command name*
- *Deleting entries*
- *Re-displaying the Current Command Line*
- *Transposing mistyped characters*
- *Controlling Capitalization*

Moving the cursor on the command line

Table 2 shows the key combinations or sequences to move the cursor on the command line. **Ctrl** defines the Control key, which must be pressed simultaneously with its associated letter key.

Esc supports the Escape key (which must be pressed first), followed by its associated letter key. Keys are not case sensitive. Specific letters are used to provide an easy way of remembering their functions. In *Table 2*, bold characters bold indicate the relation between a letter and its function.

TABLE 2 Key Combinations Used to Move the Cursor

Keystrokes	Function Summary	Function Details
Left Arrow or Ctrl-B	Back character	Moves the cursor one character to the left When entering a command that extends beyond a single line, press the Left Arrow or Ctrl-B keys repeatedly to scroll back to the system prompt and verify the beginning of the command entry. You can press the Ctrl-A key combination.
Right Arrow or Ctrl-F	Forward character	Moves the cursor one character to the right
Esc, B	Back word	Moves the cursor back one word
Esc, F	Forward word	Moves the cursor forward one word
Ctrl-A	Beginning of line	Moves the cursor to the beginning of the line
Ctrl-E	End of line	Moves the cursor to the end of the command line
Ctrl-d		Deletes the current character
Ctrl-U		Deletes text up to cursor
Ctrl-K		Deletes from the cursor to end of the line
Ctrl-P		Obtains the prior command from memory
Ctrl-N		Obtains the next command from memory
Esc-C		Converts the rest of a word to uppercase
Esc-L		Converts the rest of a word to lowercase
Esc-D		Deletes the remainder of a word
Ctrl-W		Deletes the word up to the cursor
Ctrl-Z		Enters the command and returns to the root prompt
Ctrl-L		Refreshes the input line

Completing a partial command name

If you cannot remember a command name (or if you want to reduce the amount of typing you have to perform) enter the first few letters of a command, then press the **Tab** key. The command line parser completes the command if the string entered is unique to the command mode. If your keyboard does not have a Tab key, press Ctrl-I.

The CLI recognizes a command once you have entered enough characters to make the command unique. If you enter “conf” within the privileged EXEC mode, the CLI associates the entry with the configure command, since only the configure command begins with `conf`.

In the following example, the CLI recognizes a unique string in the privileged EXEC mode when the Tab key is pressed:

```
RFController# conf<Tab>
RFController# configure
```

When using the command completion feature, the CLI displays the full command name. The command is not executed until the **Return** or **Enter** key is pressed. Modify the command if the full command was not what you intended in the abbreviation. If entering a set of characters (indicating more than one command), the system lists all commands beginning with that set of characters.

Enter a question mark (?) to obtain a list of commands beginning with that set of characters. Do not leave a space between the last letter and the question mark (?).

For example, entering `co?` lists all commands available in the current command mode:

```
RFController# co?
copy? commit
RFController# co
```

NOTE
The characters entered before the question mark are reprinted to the screen to complete the command entry.

Deleting entries

Use any of the following keys (or key combinations) to delete command entries:

Keystrokes	Purpose
Backspace	Deletes the character to the left of the cursor
Ctrl-D	Deletes the character at the cursor
Ctrl-K	Deletes all characters from the cursor to the end of the command line
Ctrl-W	Deletes a word up to the cursor
Esc, D	Deletes from the cursor to the end of the word

Re-displaying the Current Command Line

If entering a command and the system suddenly sends a message, you can recall the current command entry. To re-display the current command line (refresh the screen), use the following key combination:

Keystrokes	Purpose
Ctrl-L	Re-displays the current command line

Command output pagination

Output often extends beyond the visible screen length. For cases where output continues beyond the screen, the output is paused and a `Press Any Key to Continue (Q to Quit)` prompt displays at the bottom of the screen. To resume the output, press the Return key to scroll down one line or press the Spacebar to display the next full screen of output.

Transposing mistyped characters

If you have mistyped a command entry, you can transpose the mistyped characters. To transpose characters, use the following key combination:

Keystrokes	Purpose
Ctrl-T	Transposes the character to the left of the cursor with the character located at the cursor

Controlling Capitalization

Capitalize or lowercase words with a few simple key sequences. The controller CLI commands are generally case-insensitive (and in lowercase). To change the capitalization of the commands, use one of the following sequences:

Keystrokes	Purpose
Esc, C	Capitalizes the letters to the right of cursor
Esc, L	Changes the letters at the right of cursor to lowercase

Chapter

Common Commands

2

In this chapter

This chapter describes the CLI commands used in the USER EXEC, PRIV EXEC, and GLOBAL CONFIG modes.

The PRIV EXEC command set contains those commands available within the USER EXEC mode. Some commands can be entered in either mode. Commands entered in either USER EXEC mode or PRIV EXEC mode are referred to as EXEC mode commands. If a user or privilege is not specified, the referenced command can be entered in either mode.

Common commands

Table 2.1 summarizes available common commands:

Table 2.1 Common Commands in RFController

Command	Description	Ref.
clrscr	Clears the display screen	*page 32*
exit	Ends the current mode and moves to the previous mode	*page 33*
help	Displays the interactive help system	*page 34*
no	Negates a command or sets its defaults	*page 35*
service	Services or debugs the controller	*page 37*
show	Shows running system information	*page 59*

clrscr

Common commands

Clears the screen and refreshes the prompt (**#**)

Supported in the following platforms:

- Mobility RFS4000 Controller
- Mobility RFS6000 Controller
- Mobility RFS7000 Controller

Syntax

```
clrscr
```

Parameters

None

Example

```
RFController#clrscr
RFController#
```

exit

Common commands

Ends the current mode and moves to the previous mode

Supported in the following platforms:

- Mobility RFS4000 Controller
- Mobility RFS6000 Controller
- Mobility RFS7000 Controller

Syntax

```
exit
```

Parameters

None

Example

```
RFController(config)#exit
RFController#
```

help

Common commands

Use this command to access the advanced help feature. Use "**?**" anytime at the command prompt to access the help topic.

Two kinds of help are provided:

1. Full help is available when ready to enter a command argument.
2. Partial help is provided when an abbreviated argument is entered and you want to know what arguments match the input (for example 'show ve?').

Supported in the following platforms:

- Mobility RFS4000 Controller
- Mobility RFS6000 Controller
- Mobility RFS7000 Controller

Syntax

```
help
```

or

```
?
```

Parameters

None

Example

```
RFController>service ?
diag      Diagnostics
encrypt   Encrypt password or key with secret
kill      Kill a connection
locator   flash all LEDS to locate controller visually
save-cli  Save CLI tree for all modes in html format
show      Show running system information
undefine  Undefine non active Event Cycle spec
wireless  Wireless parameters
RFController>service
```

no

Common commands

Negates a command or sets its defaults

Supported in the following platforms:

- Mobility RFS4000 Controller
- Mobility RFS6000 Controller
- Mobility RFS7000 Controller

Syntax

```
no
```

Parameters

None

Example (User Exec)

```
RFController>no ?
 cluster-cli Cluster context
 mobile-unit  mobile-unit index
 page     Toggle paging
 service   Service Commands
RFController>no
```

Example (Priv Exec)

```
RFController#no ?
 cluster-cli Cluster context
 debug    Debugging functions
 wireless-client  wireless-client index
 page     Toggle paging
 service   Service Commands
 upgrade   Name of the patch to remove
RFController#no
```

Example (Global Config)

```
RFController(config)#no ?
 aaa             VPN AAA authentication settings
 aap-ipfilter-list   AAP ipfilter
 aap-wlan-acl    Remove an ACL from WLAN for AAP
 arp             Address Resolution Protocol
 access-list     Configure access-lists
 autoinstall     autoinstall configuration command
 banner          Reset login banner to nothing
 bridge          Bridge group commands
 country-code    Clear the currently configured country code. All existing
                 configurations will be erased
 crypto          encryption module
 errdisable      errdisable
 firewall        Wireless firewall
 ftp             Configure FTP Server
 hostname        Reset system's network name to default
 interface       Delete a virtual interface
```

```
 ip              Internet Protocol (IP)
 line            Configure a terminal line
 local           Local user authentication database for VPN
 logging       Modify message logging facilities
 mac           MAC configuration
 mac-address-table Configure MAC address table
 mac-name      Remove a configured MAC Address name
 management    sets properties of the management interface
 network-element-id Reset system's network element
 ntp           Configure NTP
 prompt        Reset system's prompt
 radius-server RADIUS server configuration commands
 ratelimit     ratelimit
 role           Configure role parameters
 redundancy    Configure redundancy group parameters
 service       Service Commands
 smtp-notification Modify SMTP-Notification parameters
 snmp-server   Modify SNMP engine parameters
 spanning-tree  Spanning tree
 timezone      Revert the timezone to default (UTC)
 traffic-shape  Traffic shaping
 username      Establish User Name Authentication
 vpn           vpn
 virtual-ip    Virtual IP
 wlan-acl      Remove an ACL from WLAN
 white-list    Host whitelist
 wlan-acl      Remove an ACL from WLAN
 wwan          Wireless WAN interface

RFController(config)#no
```

service

Common commands

Service commands are used to manage the controller configuration in all modes. Depending on the mode, different service commands will display.

Supported in the following platforms:

- Mobility RFS4000 Controller
- Mobility RFS6000 Controller
- Mobility RFS7000 Controller

Syntax(User Executable Mode)

```
service [clear|diag|encrypt|kill|locator|save-cli|show|undefine|
       wireless]
service [locator|save-cli|undefine]

service clear [command-history|reboot-history|upgrade-history]

service diag [enable|identify|limit|period|poe
       tech-support-period|tech-support-url]
service diag [enable|identify]
service diag poe debug
service diag limit [buffer|fan|filesys|inodes|load|maxFDs|
       pkbuffers|procRAM|ram|routecache|temperature]
service diag limit buffer
       [128|128k|16k|1k|256|2k|32|32k|4k|512|64|64k|8k] <0-65535>
service diag limit fan <1-3> low <1000-15000>
service diag limit filesys [etc2|flash|var]
       <limit-as-percent>
service diag limit inodes [etc2|flash|var]
       <limit-as-percent>
service diag limit load [01|05|15] <load-as-percent>
service diag limit maxFDs <0-32767>
service diag limit pkbuffers <0-65535>
service diag limit procRAM <0.0-100.0>
service diag limit ram <0.0-25.0>
service diag limit routecache <0-65535>
service diag limit temperature <temp-sensor-number> [critical|high|low]
<temperature>
service diag period <100-30000>
service diag tech-support-period <10-10080>
service diag tech-support-url <URL>

service encrypt secret 2 <passphrase> plaintext <plaintext>
service kill connection {<1-64>}

service show [cli|command-history|crash-info|diag|info|
       memory|process|reboot-history|rtls|startup-log|
       upgrade-history|watchdog]
service show [cli|command-history|crash-info|info|memory|
       process|reboot-history|startup-log|upgrade-history|
       watchdog]

service show diag [hardware|led-status|limits|period|stats|
       tech-support-period|tech-support-url|top]
```

```
service show rtls [location-history|rfid]
service show rtls location-history
service show rtls rfid events reader {<1-48>}

service undefine ecspec {<ECSpec-name>}
service wireless
```

Parameters(User Executable Mode)

clear [command-history| reboot-history| upgrade-history]	Resets functions • command-history - Clears upgrade history • reboot-history - Clears reboot history • upgrade-history - Clears upgrade history

diag [enable|identify|limit| period|poe tech-support-period| tech-support-url]	Diagnostics commands
	• enable – Enables in-service diagnostics
	• identify – Identifies a controller by flashing its LEDs
	• limit [buffer|fan|filesys|inodes|load|maxFDs| pkbuffers|procRAM|ram|routecache|temperature] – Sets the diagnostic limit command
	  • buffer []<0-65535> – Configures the buffer usage warning limit. The warning limit can be set to a buffer limit size [128|128k|16k|1k|256|2k|32|32k|4k| 512|64|64k|8k].
	  • <0-65535>– Configures buffer usage warning limit. Set between 0 and 65535.
	  • fan <1 -3> low <1000-15000> – Sets the fan speed limit for the fans on the controller.
	  • low <1000-15000> – Sets the low speed limit of the selected fan in RPMs.
	  • filesys [etc2|flash|var] – Sets the file system freespace limit
	  • inodes[etc2|flash|var] – File system inode limit
	  • load [01|05|15] – Aggregate processor load
	  • maxFDs <0-32767> – Configures the maximum number of file descriptors. Set between 0 to 32767
	  • pkbuffers <0-65535> – Configures the packet buffer head cache limit. Set between 0 and 65535.
	  • procRAM <0-100.0> – Defines the RAM space used by a process. Set the percentage <percent> of RAM space used by the processor between 0.0 and 100.0 percent.
	  • ram <0.0-25.0> – Configures free space for the RAM. Configures the free space to any value between 0.0 to 25.0 percent.

	• routecache <0-65535> – Configures IP route cache usage. Set a value between 0 and 65553.
	• temperature <1-6> [critical|high|low] – Sets the number of temperature sensors for the controller.
	  • critical <0.0 - 250.0> – Critical temperature limit
	  • high <0.0 - 250.0> – high temperature limit
	  • low <0.0 - 250.0> – low temperature limit
	• period <100-30000> – Configures the diagnostics period. Set a value between 100-30000 milliseconds. The default value is 1000 milliseconds.
	• poe debug - Power over Ethernet
	  • debug - Enables debugging
	• tech-support-period <10-10080> – Sets diagnostics tech-support-period
	  • <10-10080> – The default 1440 minutes (1 day)
	• tech-support-url <URL>– Set the URL to use during auto generated technical support dumps
	  • <URL> – URL to which to copy
	  • tftp://<hostname|IP>[:port]/path/file
	  • ftp://<user>:<passwd>@<hostname|IP>[:port]/path/file
	  • sftp://<user>@<hostname|IP>[:port]>/path/file

encrypt secret 2 <pass-phrase> plaintext <plain-text>	Encrypts a password or key with a secret passphrase • secret – Encrypts passwords/keys with a secret phrase • 2 – Type of encryption SHA256-AES256 • <pass-phrase> – Defines the passphrase used for encryption • <plain-text> – Defines the plain text password or key to encrypt
kill connection ***{<1-64>}***	Kills a connection using ESPI Adapter index • connection *{<1-64>}* – A single optional ESPI Adapter index <1-64>
locator	Locates the controller by flashing all LEDs.
save-cli	Saves the CLI tree for all modes in HTML

show [cli|command-history|crash -info|diag| info|memory|process| reboot-history|rtls| startup-log| upgrade-history| watchdog]	Displays running system information
	• cli – Shows the CLI tree of the current mode
	• command-history – Displays the command (except show commands) history
	• crash-info – Displays information about core, panic and AP dump files
	• diag [hardware|led-status|limits|period|stats |tech-support-period|tech-support-url|top] – Sets or displays controller diagnostics
	  • hardware – Shows the system hardware configuration
	  • led-status – Shows LED state variables and the current state
	  • limits – Shows limit values
	  • period – Shows the period (ms) for in-service diagnostics
	  • stats – Shows current diagnostics statistics
	  • top – Shows the top processes (sorted by memory usage)
	  • tech-support-period <10-10080> – Shows diagnostics tech-support-period
	  • <10-10080> – The default 1440 minutes (1 day)
	  • tech-support-url <URL> –Shows the URL to use during auto generated technical support dumps
	  • <URL> – URL to which to copy
	  • tftp://<hostname|IP>[:port]/path/file
	  • ftp://<user>:<passwd>@<hostname|IP>[:port]/path /file
	  • sftp://<user>@<hostname|IP>[:port]>/path/file

	info – Shows a snapshot of available support information
	• memory – Shows memory statistics
	• watchdog – Shows watchdog status
	• process – Shows processes (sorted by memory usage)
	• reboot-history – Shows a reboot history
	• startup-log – Shows the startup log
	• upgrade-history – Shows an upgrade history
	• rtls [location-history|rfid] – Real Time Locationing System commands
	  • location-history – Show location engine history
	  • rfid events – RFID Configuration
	  • events reader – RFID reader events
	  • reader <1-48> – A single RFID reader index
	• watchdog – Shows watch dog status

undefine ecspec ***{<SPECNAME>}***	Undefines non active Event Cycle Specification • ecspec *{<SPECNAME>}* – Name of optional ECSpecs configuration
wireless	Displays current wireless parameters

Syntax (Privilege Executable Mode) (Priv Exec)

```
service [clear|copy|diag|
        diag-shell|encrypt|firewall|ip|kill|locator|pktcap|pm|
        save-cli|securitymgr|show|smart-rf|start-shell|undefine|
        watchdog|wireless]
service [diag-shell|locator|pm stop|save-cli|start-shell|
        watchdog]
```

```
service clear [all|aplogs|clitree|cores|dumps|fw|panics|
       snooptable|securitymgr|wireless]
service clear fw flows
service clear securitymgr flows [<flow-index>|<interface>|
       all|ge <ge-index>|me1|sa <sa-index>|vlan <vlan-id>]

service copy tech-support [<file>|<URL>] [tftp|ftp|sftp]

service diag [enable|identify|limit|period|
       tech-support-period|tech-support-url]

service encrypt secret 2 <pass-phrase> <plain-text>
service firewall disable
service firewall ip igmp snooping robustness-variable <1-7>
service kill conncection {<1-64>}

service pktcap on [bridge|deny|drop|interface|router|vlan]
service pktcap on [bridge|drop] {[count <1-1000000>|filter|hex|snap
<1-1518>|verbose|write]}
service pktcap on bridge filter on
       [<LINE>|arp|capwap|dst|ether|host|icmp|igmp|ip|ip6|l2|l3|
       l4|net|not|port|src|tcp|udp|vlan|wlan]
service pktcap on bridge filter [arp|capwap|icmp|ip|ip6|
       igmp|udp] {[and|or]
       <LINE>}
service pktcap on bridge filter capwap {[ctrl|data] [and|or] <LINE>}
service pktcap on bridge filter dst [A.B.C.D|net|port]
       {[and|or] <LINE>}
service pktcap on bridge filter ether [broadcast|dst|host|
       multicast|proto|src]
service pktcap on bridge filter ether [broadcast|multicast]
       {[and|or] <LINE>}
service pktcap on bridge filter ether [dst|host|src] <MAC>
       {[and|or] <LINE>}
service pktcap on bridge filter ether proto <0-65535>
       {[and|or] <LINE>}
service pktcap on bridge filter ether host <IP> {[and|or] <LINE>}
service pktcap on bridge filter ip multicast {[and|or] <LINE>}
service pktcap on bridge filter ip proto [<0-255>|
<protocol>] {[and|or] <LINE>}
service pktcap on bridge filter [l2|l3|l4] [u16 <0-126>|
u32 <0-124>|u8 <0-127>]
service pktcap on bridge filter net <IP/MASK> {[and|or] <LINE>}
service pktcap on bridge filter not [arp|capwap|dst|ether|
       host|icmp|igmp|ip|ip6|l2|l3|l4|net|not|port|src|tcp|udp|
       vlan|wlan]
service pktcap on bridge filter port <0-65535> {[and|or] <LINE>}
service pktcap on bridge filter src [<IP>|net <IP/MASK>|
       port <0-65536>] {[and|or] <LINE>}
service pktcap on bridge filter tcp {[[and|or] <LINE>|[ack|fin|or|rst|syn]
{[and|or] <LINE>]}
service pktcap on bridge filter vlan <1-4095> {[and|or] <LINE>}
service pktcap on bridge filter wlan <1-2> {[and|or] <LINE>}
service pktcap on bridge [hex|verbose] {[count <1-1000000>|
       filter [...] |snap <1-1518>]}
service pktcap on bridge snap <1-1518> {filter [...]}
service pktcap on bridge write [<FILE>|<URL>]
       {[count <1-1000000>|filter [...] |snap <1-1518>]}
```

```
service pktcap on deny [access-list|count|filter|
       hex|inbound|outbound|snap|verbose|write]
service pktcap on deny access-list <ACL-index> {[and|or]
       <LINE>}
service pktcap on deny [inbound|outbound] {[access-list|
       count|filter|hex|[inbound|outbound]|snap|verbose|write]}
       {[and|or] <LINE>}
service pktcap on interface [<INTERFACE>|ge <1-4>|me1|
       sa <1-4>|vlan <1-4094>] {[count|filter|hex|inbound|
       outbound|snap|verbose|write]} {[and|or] <LINE>}
service pktcap on router {[count|filter|hex|snap|verbose|
       write]} {[and|or] <LINE>}
service pktcap on vpn {[count|filter|hex|inbound|outbound|
       snap|verbose|write]} {[and|or] <LINE>}

service securitymgr [disable|disable-flow-rate-limit|
       dump-core|enable-http-stats|tftplag]

service show [cli|command-history|crash-info|diag|fw|info|
ip|last-passwd|memory|pm|process|reboot-history|rtls|
securitymgr|smart-rf|startup-log|upgrade-history|watchdog|
wireless]
service show [cli|command-history|crash-info|diag|info|
       memory|process|reboot-history|rtls|startup-log|
       upgrade-history|watchdog]

service show fw flows brief
service show ip igmp snooping vlan <1-4094> {<MULTICAST-IP>}
service show last-passwd
service show pm {history [<process-name>|all]

service show rtls [grid|location-history|rfid]
service show rtls grid [all|x]
service show rtls grid all
service show rtls grid x <0-9000> y <0-9000>
service show rtls rfid events reader {<1-48>}

service show securitymgr flows [details|source]
service show securitymgr flows details {source [<IP>|any]
       destination [<IP>|any] protocol [any|icmp|tcp|udp]}
service show securitymgr flows source [<IP>|any] destination [<IP>|any]
protocol [any|icmp|tcp|udp]

service show smart-rf [debug-config|sensitivity]
service show smart-rf debug-config
service show smart-rf sensitivity [client|pattern|rates]
service show smart-rf sensitivity client {<1-8192>|<MAC>}
service show smart-rf sensitivity pattern
[pattern-11a|pattern-11b|pattern-11bg|pattern-2-mbps]

service show wireless [ap-history|buffer-counters|
       enhanced-beacon-table|enhanced-probe-table|group|
       group-stats|legacy-load-balance|client-cache-buckets|
       client-cache-entry|mvlan|radio|radio-cache-entry|
       radio-hash-buckets|snmp-trap-throttle|vlan-cache-buckets|
       vlan-cache-entry|waiting]
service show wireless [buffer-counters|group-stats|
       legacy-load-balance|client-cache-buckets|radio-hash-buckets|
       snmp-trap-throttle|vlan-cache-buckets]
```

```
service show wireless ap-history <MAC>
service show wireless[enhanced-beacon-table|
       enhance-probe-table] [config|report]
service show wireless group <1-256>
service show wireless client-cache-entry {<1-8192>|<MAC>}
service show wireless mvlan <1-256>
service show wireless radio [<1-4096>|description|mapping]
service show wireless radio-cache-entry {<MAC>}
service show wireless vlan-cache-entry {[<1-8192>|<MAC>]}
service show wireless waiting {<1-99>}

service smart-rf
[clear-history|load-from-file|replay|rescue|restore|save-to-file|simulate]
service smart-rf replay enable
service smart-rf [rescue|restore] [<radio-mac>|
       <radio-index>|<radio-index-list>]
service smart-rf simulate [coverage-hole|interference]
service smart-rf simulate coverage-hole <1-4096>
       <unit-range> [<unit-range>|pattern-11a|pattern-11b|
       pattern-11bg|pattern-2-mbps]
service smart-rf interference [<radio-mac>|<radio-index>|
       <radio-index-list>]

service undefine ecspec {<SPECNAME>}

service wireless [ap-history|clear-ap-log|custom-cli|dot11i|
       dump-core|enhanced-beacon-table|enhanced-probe-table|
       free-packet-watermark|idle-radio-send-multicast|
       legacy-load-balance|map-radios|radio-misc-cfg|rate-scale|
       request-ap-log|save-ap-log|snmp-trap-throttle|
       sync-radio-entries|vlan-cache]
service wireless [dumpcore|legacy-load-balance|rate-scale|
       save-ap-log|sync-radio-entries]
service wireless ap-history [clear|enable]
service wireless clear-ap-log {<1-1024>}

service wireless custom-cli [sh-wi-wireless-client|sh-wi-radio]
service wireless custom-cli sh-wi-wireless-client [ap-locn|
       ap-name|channel|dot11-type|ip|last-heard|mac|radio-bss|
       radio-desc|radio-id|ssid|state|vlan|wlan-desc|wlan-id|
       username]
service wireless custom-cli sh-wi-radio [adopt-info|
       ap-locn|ap-mac|ap-name|bss|channel|dot11-type|num-client|
       power|radio-desc|radio-id|state]

service wireless dot11i enforce pmkid-validation

service wireless enhanced-beacon-table [channel-set|enable|
       erase-report|max-ap|scan-interval|scan-time]
service wireless enhanced-beacon-table [enable|erase-report]
service wireless enhanced-beacon-table channel-set
       [a|an|bg|bgn] <1-200>
service wireless enhanced-beacon-table max-ap <0-512>
service wireless enhanced-beacon-table scan-interval <10-60>
service wireless enhanced-beacon-table scan-time <100-1000>

service wireless enhanced-probe-table
[enable|erase-report|max-client|preferred|window-time]
service wireless enhanced-probe-table [enable|erase-report]
service wireless enhanced-probe-table max-client <0-512>
```

```
service wireless enhanced-probe-table preferred <MAC>
service wireless enhanced-probe-table window-time <10-60>

service wireless free-packet-watermark <0-100>
service wireless idle-radio-send-multicast enable
service wireless map-radios <1-127>
service wireless radio-misc-cfg <hex-mask>
service wireless request-ap-log <ap-index>
service wireless snmp-trap-throttle <1-20>
service wireless vlan-cache enable
```

Parameters (Privilege Executable Mode)

clear [all|aplogs|clitree|cores|dumps|fw|panics|snooptable|wireless]	Performs a variety of reset functions
	• all – Removes all core, dump and panic files
	• aplogs – Removes all AP log files
	• clitree – Removes clitree.html (created by the save-cli command)
	• cores – Removes all core files
	• dumps – Removes all dump files
	• fw flows – Clears firewall sessions
	  • flows – Firewall established sessions
	• panics – Removes all kernel panic files
	• securitymgr flows – Securitymgr parameters
	  • flows [<0-349>|ge me1|sa|vlan|all] – Sessions established
	  • <0-349> – Flow Index
	  • WORD – Interface name
	  • all – All established sessions
	  • vlan <1-4094> – VLAN
	  • me1 - Fast Ethernet interface
	  • sa <1-4> – Static Aggregate interface
	  • ge <1-4> – Gigabit Ethernet interface
	• snooptable – Clear Static and Dynamic Snoop entries
	• wireless – wireless related parameters
	  • wireless-client association-statistics– Clears wireless client related parameters
	  • association-statistics – Clears association and reassociation statistics

copy tech-support [<file>|<URL>] [tftp|ftp|sftp]	Copies files for tech support purposes
	• tech-support [<file>|<URL>] [tftp|ftp|sftp] – Copies extensive system information useful to technical support for troubleshooting.
	  • FILE – File to which to copy
	  • cf:/path/file
	  • usb1:/path/file
	  • usb2:/path/file
	  • URL– Target URL from which to copy
	  • tftp://<hostname:port or IP>/path/file
	  • ftp://<user>:<passwd>@<hostname:port or IP>/path/file
	  • sftp://<user>@<hostname:port or IP>/path/file

dhcp-snoop-conflict-detection disable	IP Address, MAC Address conflict detection based on DHCP Snoop Table • disable – Disable packet drop based on conflict detection

diag [enable|identify|limit|period|tech-support-period|tech-support-url]	Sets or displays controller diagnostic values
	• enable – Enables in-service diagnostics
	• fanduty <40-100> – CPU fan PWM duty cycle. Set a value between 40-100%. Setting a value below 60 is considered unreliable.
	• identify – Identifies a controller by flashing the LEDs
	• limit [buffer|fan|filesys|inodesload|maxFDs |pkbuffers|procRAM|ram|routechache|temperature] – Diagnostic limit commands
	  • buffer [] – Configures the buffer usage warning limit. The warning limit can be set to the buffer limit size of [128|128k|16k|1k|256|2k|32|32k|4k|512|64|64k|8k]
	  • fan <1-3> low <1000-150000> – Sets the fan speed limit for the fans on the controller.
	  • low <1000-15000> – Sets limit value from 1000 to 15000
	  • filesys [etc2|flash|var] – Sets the file system freespace limit
	  • inodes [etc2|flash|var] – Sets the file system inode limit
	  • load [01|10|15] – Aggregate processor load
	  • maxFDs <0-32767> – Configures the maximum number of file descriptors between 0 - 32767.
	  • pkbuffers <0-65535>– Sets the packet buffer head cache limit between 0 - 65535.
	  • procRAM <0.0-100.0> – Configures the RAM space used by a process. Set the percentage of RAM space between 0.0 and 100.0 percent .
	  • ram <0.0-25.0> – Configures the free space for the RAM. Configure the free space between 0.0 and 25.0 percent.

	• routecache <0-65535> – Configures IP route cache usage. Set between 0 and 65553.
	• temperature <1-6> [critical|high|low] – Sets the number of temperature sensors for the controller.
	  • critical <0.0 - 250.0> – Critical temperature limit
	  • high <0.0 - 250.0> – high temperature limit
	  • low <0.0 - 250.0> – low temperature limit
	• period <100-30000> – Configures the diagnostics period. Set a value between 100-30000 milli seconds. The default value is 1000 milliseconds

diag-shell	Provides diag shell access
encrypt[secret|2|<pass-phrase>|<encryption-key>]	Encrypt password or key with secret • secret – Encrypt passwords/keys with secret phrase • 2 – Type of encryption SHA256-AES256 • <pass-phrase> – Passphrase for encryption • <encryption-key> – Plaintext password or key to encrypt
firewall disable	Configures firewall parameters • disable – Disable firewall
kill connection *{<1-64>}*	Kills a connection using ESPI Adapter index • connection <1-64> – A single optional ESPI Adapter index

pktcap on [bridge|interface|router|vpn] [count|filter|verbose|write]	Packet capturing
	• on – Defines the packet capture location
	• bridge [count|hex|snap|verbose|write|filter] – Captures packet at the bridge
	  • count <1-1000000> – Limits the captured packet count
	  • filter [<LINE>|arp|capwap|dst|ether|host|icmp|igmp|ip|ip6|l2|l3|l4|net|not|port|src|tcp|udp|vlan|wlan] – Filters packets based on specified criteria.
	  • <LINE> – Defines user defined packet capture filter
	  • arp – Match arp packets
	  • capwap – Match Capwap packets
	  • dst – Match IP destination
	  • ether – Ethernet
	  • host – Match IP address
	  • icmp – Match icmp packets
	  • igmp – Match igmp packets
	  • ip – Match IPV4 packets
	  • ip6 – Match IPV6 packets
	  • l2 – Match L2 header
	  • l3 – Match L3 header
	  • l4 – Match L4 header
	  • net – Match IP in subnet
	  • not – Logical not
	  • port – Match TCP or UDP port
	  • src – Match IP source
	  • tcp – Match TCP packets
	  • udp – Match UDP packets
	  • vlan – Match vlan
	  • wlan – Match wlan

	• verbose <1-1000000> – Displays full packet body • filter – Captures the filter • snap <1-1518>– Captured data length • write [<FILE>|URL] – Captures to a file • FILE – File to which to copy • cf:/path/file • usb1:/path/file • usb2:/path/file • URL– Target URL from which to copy • tftp://<hostname:port or IP>/path/file • ftp://<user>:<passwd>@ <hostname:port or IP>/path/file • sftp://<user>@<hostname:port or IP>/path/file • interface [<WORD>|ge|me1|sa|vlan] – Captures at an interface • WORD – Interface name • ge <1-4> – Gigabit Ethernet interface • me1 – Fast Ethernet interface • sa <1-4> – Static Aggregate interface • vlan <1-4094> – VLAN • count – Limits capture packet count • filter – Filters on criteria • inbound – Captures inbound packets only • outbound – Captures outbound packets only • verbose – Displays full packet body • write – Captures to a file • snap – Captured data length • hex – Show full packet body • router [counter|filter|verbose|write|snap|hex] – Captures packets at the router.
	• count <1-1000000> – Limits capture packet count • filter – Captures filter • verbose – Displays full packet body • write – Captures to a file • snap <1-1518> – Captured data length • hex – Show full packet body • count – Limits capture packet count • filter – Captures the filter • snap – Captured data length • vpn – Captures at the VPN • count – Limits capture packet count • filter – Captures the filter • inbound – Captures ingress direction only • outbound – Captures egress direction only • verbose – Displays full packet body • write – Captures to a file • snap – Captured data length • hex – Show full packet body • count – Limits capture packet count • filter – Captures the filter • snap – Captured data length
pm stop	Process Monitor • stop – Stops the PM from monitoring all daemons

save-cli	Saves the CLI tree for all modes in HTML
securitymgr [disable| disable-flow-rate-limit| dump-core| enable-http-stats]	Securitymgr parameters • disable – Disables securitymgr • disable-flow-rate-limit – Disables flow rate limiting • dump-core – Creates a core file of the securitymgr process • enable-http-stats – Enables the securitymgr HTTP statistics interface

show [cli| command-history| crash-info|diag|fw|info| ip|last-passwd|memory| pm|process| reboot-history|rtls| securitymgr|smart-rf| startup-log| upgrade-history| watchdog|wireless]	Displays running system information
	• cli – Shows the CLI tree of the current mode
	• command-history – Displays a command (except show commands) history
	• crash-info – Displays information about core, panic and AP dump files
	• diag [hardware|period|limits|stats|tech-support-period| tech-support-url|top] – Displays diagnostics
	  • hardware – Displays the hardware system configuration
	  • period – Displays the period (ms) for the in service diagnostics
	  • limits – Displays limits value
	  • stats – Displays current diagnostics statistics
	  • tech-support-period – Displays the tech-support period (minutes) for the in service diagnostics
	  • tech-support-url – Displays the tech-support-url
	  • top –Displays top processes
	• fw flows – Firewall
	  • flows brief– Sessions Established
	  • brief – Summary of active flows
	• info – Shows a snapshot of available support information
	• last-passwd – Displays the last password used to enter the shell
	• memory – Shows memory statistics

	• pm history – Process Monitor
	  • history [WORD|all] – Displays state changes for a process, the time they happened and events
	  • WORD – Process name
	  • all – All processes
	• process – Shows processes (sorted by memory usage)
	• reboot-history – Shows a reboot history
	• rtls [grid|location-history|rfid] – Locationing Configuration
	  • grid [all|x] – Displays RSSI values in grid
	  • all – Displays all grids
	  • x <0-9000> – Displays grid x coordinates
	  • y<0-9000> – Displays grid y coordinates
	  • location-history [events] – Displays location engine history
	  • rfid [events]– RFID Configuration
	  • events <1-48> – Displays RFID reader events
	  • <1-48> – A single RFID reader index
	• securitymgr – Security manager information displays
	• smart-rf [debug-config| sensitivity] – Smart-RF Management commands
	  • debug-config – Displays smart-rf debug configuration
	  • sensitivity [client|pattern|rates] – Displays sensitivity table
	  • client[<1-8192>|WORD]– for given client
	  • <1-8192> – A single index
	  • WORD – MAC address of client-cache entry to show
	  • pattern|rates – for common client pattern
	• startup-log – Shows the startup log
	• upgrade-history – Shows an upgrade history
	• watchdog – Shows the watchdog status
	• wireless – Displays wireless parameters

show securitymgr flows	Service Security Manager parameters
	• flows [details|source] – Sessions established
	  • details – Shows detail flow statistics
	  • source [A.B.C.D|any] – Shows the source IP address
	  • [A.B.C.D|any] – Flows where source address is A.B.C.D or flows with any source address
	  • destination [A.B.C.D|any] – Destination IP address
	  • [A.B.C.D|any] – Flows where the destination address is A.B.C.D or flows with any destination address
	  • protocol [any|icmp|tcp|udp] – Protocol type
	  • [any|icmp|tcp|udp] – Flows having any or icmp or tcp or udp protocol

smart-rf [clear-history|load-from-file|replay|rescue|restore|save-to-file|simulate]	Displays Smart-RF Management Commands
	• clear-history– clears assignment history
	• load-from-file – load record from file
	• replay enable – set replay mode
	  • enable – enable replay mode
	• rescue <MAC> – force rescue operation
	  • <MAC> – A single radio-mac-address, a single index
	• restore <MAC> – remove any recovering operation on given mode
	  • <MAC> – A single radio-mac-address a single index
	• save-to-file – save records to file smart.bin
	• simulate [coverage-hole|interference] – Simulate radio events
	  • coverage-hole <1-4096> – Simulate coverage hole
	  • experienced-rate transmit-rate – Provide the experienced rate in mbps
	  • transmit-rate [patter-11a|pattern-11b|pattern-11bg|pattern-2-mbps] – Provide the simulated clients's allowed transmit rates in hexadecimal format
	  • pattern-11a – 11a Unit
	  • pattern-11b – 11b Unit
	  • pattern-11bg – 11bg Unit
	  • pattern-2-mbps – 2 Mbps Unit
	  • interference <MAC> – Simulate interference on radio
	  • <MAC> – A single radio-mac-address, a single index

start-shell	Provides shell access
test	Provides test parameters
undefine ecspec <SPECNAME>	Undefines non active Event Cycle Specification • ecspec <SPECNAME> – Name of ECSpecs configuration
watchdog	Enables the controller watchdog

wireless [ap-history|
clear-ap-log
|custom-cli|dot11i|
dump-core|
enhanced-beacon-table|
enhanced-probe-table|
free-packet-watermark
|idle-radio-send-multicast|
legacy-load-balance
|map-radios|
radio-misc-cfg
|rate-scale|
request-ap-log
|save-ap-log
|snmp-trap-throttle|
sync-radio-entries|
vlan-cache]
	Wireless parameters
	• ap-history [clear|enable] – Access-point history
	  • clear – Delete all history of all APs
	  • enable – Enable the tracking of AP history
	• clear-ap-log <1-1024> – Clears the AP logs
	• custom-cli [sh-wi-wireless-client|sh-wi-radio] – Customize the output of some summary cli commands in wireless
	  • sh-wi-wireless-client [ap-locn|ap-name|channel|dot11-type|ip|last-heard|mac|radio-bss|radio-desc|radio-id|ssid|state|username|vlan|wlan-desc|wlan-id|username] – Customize the output of the "show wireless wireless-client' command
	  • ap-locn – The location of the AP where the wireless-client is associated
	  • ap-name – The name of the AP where the wireless-client is associated
	  • channel – The channel of the radio where the wireless-client is associated
	  • dot11-type –The dot11 radio type of the wireless-client
	  • ip – The IP address of the wireless-client
	  • last-heard – the time when a packet was last received from the wireless-client
	  • mac – MAC address of wireless-client
	  • radio-bss – the bssid of the radio where the wireless-client is associated

- radio-desc – description of radio where the wireless-client is associated
- radio-id – The radio index to which the wireless-client is associated
- ssid – The ssid of the wireless-clients wlan
- state – The current state of the wireless-client
- username – The Radius username of the user connected through this device (shown only if applicable and available)
- vlan – The vlan-id assigned to the wireless-client
- wlan-desc – The wlan description the wireless-client is using
- wlan-id – The wlan index the wireless-client is using

- sh-wi-radio [adopt-info|ap-locn|ap-mac|ap-name|bss|channel|dot11-type|num-client|power|radio-desc|radio-id|state] – Customize the output of the "show wireless radio" command
  - adopt-info – The adoption information about the radio
  - ap-locn – The location of the AP to which this radio belongs
  - ap-mac – The MAC address of AP to which the radio belongs
  - ap-name – The name of the AP to which this radio belongs
  - bss – The bssid of the radio
  - channel –The configured and current channel of the radio
  - dot11-type – The the dot11 type (11a/11g etc) of the radio

- num-client – The number of mobile devices associated with this radio
- power – The configured and current transmit power of the radio
- pref-id – The adoption preference id of the radio
- radio-desc – The description of the radio
- radio-id – The radio index in configuration
- state – The current operational state of the radio

- dot11i – modify dot11i service parameters
- dump-core – Creates a core file of the ccsrvr process
- enhanced-beacon-table [channel-set|enable|erase-report|max-ap|scan-interval|scan-time]– Enhanced beacon table for AP locationing.
  - channel-set [a|an|b|bg|bgn] <1-200> – Adds channels to the different radio types. Channel types are a, an, b, bg, bgn. The channel number must be in the range 1 to 200.
  - enable – Enables the Enhance Beacon Table feature for AP locationing
  - erase-report – Erases the reports for Enhanced Beacon Table feature.
  - max-ap <0-512> – Sets the maximum number of APs to be recorded in the Enhanced Beacon Table. Set a value in the range 0 -512.
  - scan-interval <10-60>– The time duration between two enhanced beacon table for AP locationing scans in seconds.
  - scan-time <100-1000>– The time duration of an Enhanced Beacon Table scan in millisecond.s

	• enhanced-probe-table [enable|erase-report|max-client|preferred|window-time] – Enhanced probe table for Client locationing.
	  • enable – Enables the Enhanced Probe Table feature for Client locationing.
	  • erase-report – Erases the reports for Enhanced Probe Table feature.
	  • max-client <0-512> – Sets the maximum clients in the Enhance Probe Table report.
	  • preferred <MAC> – Add the MAC <MAC> to the preferred Client list.
	  • window-time – Sets the Window Time for probe collection in seconds to a value in the range 10 to 60 seconds.

	• free-packet-watermark – It is free packets threshold. If the percentage of free packets is lower than this number, then additional packets will not be queued up in the datapath • idle-radio-send-multicast – Forward multicast packets to radios without associated wireless clients • legacy-load-balance – Invoke legacy load balance algorithm • map-radios – Set radio-to-cpu mapping constant • radio-misc-cfg – radio specific misc configuration U16 for all radios • rate-scale – Enable wireless rate scaling (default) • request-ap-log – Request ap Log • save-ap-log – Saves debug/error logs sent by the access-point • snmp-trap-throttle – Limits the number of SNMP traps generated from the wireless module • sync-radio-entries – sync radio configuration at cluster levels • vlan-cache – VLAN-cache mode

Syntax (Global Config Mode) (Global Config)

```
service [advanced-vty|dhcp|diag|password-encryption|pm|
       prompt|radius|redundancy|set|show|terminal-length|
       watchdog]
service [advanced-vty|dhcp|watchdog]

service diag [enable|limit|period|tech-support-period|
       tech-support-url]
service password-encryption secret 2 <pass-phrase>
service pm sys-restart
service prompt crash-info
service radius {restart}
service redundancy dynamic-ap-load-balance start
service set [command-history|reboot-history|upgrade-history]
       <10-100>
service show cli
service terminal-length <0-512>
```

Parameters (GLOBAL Config)

advanced-vty	Enables advanced mode vty interface
dhcp	Enables the DHCP server
diag[enable|limit|period| tech-support-period| tech-support-url]	Displays diagnostics • enable – Enables in-service diagnostics • limit – Diagnostic limit command • period – Sets the diagnostics period • tech-support-period – Sets diagnostics tech-support-period • tech-support-url – Sets the URL to use during auto generated technical support dumps
password-encryption [secret|2|<pass-phrase> |<encryption-key>]	Encrypts passwords • secret – Encrypts passwords/keys with a secret phrase • 2 – Type of encryption SHA256-AES256 • <pass-phrase> – Passphrase for encryption • <encryption-key> – Plaintext password or key to encrypt
pm sys-restart	Process Monitor • sys-restart – Enables the PM to restart the system when a processes fails
prompt crash-info	Enable crash-info prompt • crash-info – Enables a crash-info prompt
radius restart	Enable radius server • restart – Restarts the radius server with an updated configuration
redundancy dynamic-ap-load-balance start	Configure redundancy group parameters • dynamic-ap-load-balance start – Enables the Dynamic AP Load Balance feature • start – Start dynamic AP load balance
set [command-history |reboot-history| upgrade-history]	Set service parameters. • command-history <10-300> – Sets the size of the command history (default is 200) • reboot-history <10-100> – Sets the size of the reboot history (default is 50) • upgrade-history <10-100> – Sets the size of the upgrade history (default is 50)
show	Shows running system information • cli – Shows the CLI tree of the current mode
terminal-length <0-512>	System wide terminal length configuration • <0-512> – Number of lines of VTY (0 means no line control)
watchdog	Enables the watchdog

Usage Guidelines

The `service password-encryption` set by the user cannot be disabled without knowing the old password. Refer the note below for more clarification.

NOTE

The `no service password-encryption` command used to disable the encryption, now requires the user to know the old password. The user will have to enter the old password to disable the encryption.

Earlier, using `no service password-encryption` disabled the encryption and `show running config` displayed the passwords as plaintext.

Now, the user has to user `no service password-encryption <old password key>` to disable or change the password.

Example

```
RFController#service diag ?
 enable              Enable in service diagnostics
 identify             Identify this controller by flashing the LEDs in a
                     rapidly changing pattern
 limit               diagnostic limit command
 period              Set diagnostics period
 tech-support-period Set diagnostics tech-support period
 tech-support-url     Set the URL to use during auto generated technical
                      support dumps

RFController#service diag enable

RFController#service diag limit ?
 buffer    buffer usage warning limit
 fan     Fan speed limit
 filesys   file system freespace limit
 load     agregate processor load
 maxFDs    maximum number of file descriptors
 pkbuffers  packet buffer head cache
 procRAM   percent RAM used by a process
 ram     percent free RAM
 routecache  IP route cache usage
 temperature temperature limit

RFController#service diag limit buffer ?
 128  128 byte buffer limit
 128k 128k byte buffer limit
 16k  16k byte buffer limit
 1k  1k byte buffer limit
 256  256 byte buffer limit
 2k  2k byte buffer limit
 32  32 byte buffer limit
 32k  32k byte buffer limit
 4k  4k byte buffer limit
 512  512 byte buffer limit
 64  64 byte buffer limit
 64k  64k byte buffer limit
 8k  8k byte buffer limit


RFController>service show command-history

Configured size of command history is 200

 Date & Time     User Location  Command
============================================================
May 31 21:57:44 2010  admin   vty 130   exit
```

```
May 31 20:30:11 2010  admin   vty 130   configure terminal
May 31 20:27:08 2010  admin   vty 130   enable
May 31 20:18:03 2010  admin   vty 130   exit
May 31 20:17:32 2010  admin   vty 130   configure terminal
May 31 20:17:26 2010  admin   vty 130   enable
May 31 18:32:42 2010  admin   con 0   ip address 10.10.10.2/24
May 31 18:32:29 2010  admin   con 0   interface vlan 1
May 31 18:31:48 2010  admin   con 0   configure terminal
May 31 18:31:45 2010  admin   con 0   enable
May 29 15:40:04 2010  admin   vty 131  enable
May 29 15:23:43 2010  admin   con 0   exit
May 29 15:23:36 2010  admin   con 0   ip address 10.10.10.2/24
May 29 15:23:19 2010  admin   con 0   exit
May 29 15:23:19 2010  admin   con 0   exit
May 29 15:23:03 2010  admin   con 0   interface vlan 1
May 29 15:22:48 2010  admin   con 0   configure terminal
May 29 15:22:45 2010  admin   con 0   enable
May 25 21:32:27 2010  admin   vty 131   configure terminal
May 25 21:32:21 2010  admin   vty 131   enable
May 24 18:34:36 2010  admin   vty 131   configure terminal
May 24 18:34:21 2010  admin   vty 131   enable
May 23 19:07:35 2010  admin   vty 131   configure terminal
May 23 19:06:59 2010  admin   vty 131   enable
May 23 14:36:09 2010  admin   vty 130   enable
May 21 16:37:13 2010  admin   vty 130   enable
May 21 16:34:36 2010  admin   con 0    enable

RFController>service show reboot-history
Configured size of reboot history is 50

 Date & Time       Event
====================================================
May 31 18:29:42 2010   startup
- - -          shutdown (ungraceful:unexpected cold restart)
May 31 15:42:23 2010   startup
- - -          shutdown (ungraceful:unexpected cold restart)
May 31 12:35:18 2010   startup
- - -          shutdown (ungraceful:unexpected cold restart)
May 30 17:15:13 2010   startup
- - -          shutdown (ungraceful:unexpected cold restart)
May 29 15:10:51 2010   startup
- - -          shutdown (ungraceful:unexpected cold restart)
May 28 20:06:31 2010   startup
- - -          shutdown (ungraceful:unexpected cold restart)
May 25 14:21:35 2010   startup
- - -          shutdown (ungraceful:unexpected cold restart)
May 24 14:20:09 2010   startup
- - -          shutdown (ungraceful:unexpected cold restart)
May 23 14:07:21 2010   startup
- - -          shutdown (ungraceful:unexpected cold
```

show

Common commands

Displays the settings for the specified system component. There are a number of ways to invoke the show command:

- When invoked without any arguments, it displays information about the current context. If the current context contains instances, the show command (usually) displays a list of these instances.
- When invoked with the display_parameter, it displays information about that component.

Supported in the following platforms:

- Mobility RFS4000 Controller
- Mobility RFS6000 Controller
- Mobility RFS7000 Controller

Syntax

```
show <parameter>
```

Parameters

Display Parameters	*Description*	*Mode*	*Example*
autoinstall	Displays the autoinstall configuration	Common	*page 62*
banner	Displays the message of the day login banner	Common	*page 63*
commands	Displays command lists	Common	*page 64*
crypto	Displays current encryption details	Common	*page 65*
environment	Displays environmental information	Common	*page 68*
history	Displays the session command history	Common	*page 68*
interfaces	Displays the current interface status and configuration	Common	*page 69*
ip	Displays the internet protocol	Common	*page 71*
ldap	Displays the LDAP server configuration	Common	*page 76*
licenses	Displays the installed licenses, if any	Common	*page 77*
logging	Displays the logging configuration and buffer	Common	*page 78*
mac	Displays the media access control IP configuration	Common	*page 79*
mac-address-table	Displays the MAC address table	Common	*page 80*
management	Displays L3 management interface name	Common	*page 81*
mobility	Displays mobility parameters	Common	*page 82*
ntp	Displays network time protocol information	Common	*page 84*
port-channel	Displays port channel commands	Common	*page 85*
power	Displays power over ethernet command	Common	*page 86*
privilege	Displays the current privilege level	Common	*page 87*

Display Parameters	Description	Mode	Example
radius	Displays RADIUS configuration commands	Common	*page 88*
redundancy dynamic-ap-load-balance	Display configuration details for dynamic AP Load Balance	Common	*page 89*
redundancy group	Displays redundancy group parameters	Common	*page 90*
redundancy history	Displays the state transition history of the controller	Common	*page 92*
redundancy members	Displays redundancy group members in detail	Common	*page 93*
rtls	Displays *Real Time Location System* (RTLS) commands	Common	*page 94*
smtp-notification	Displays trap enable flags (new)	Common	*page 97*
snmp	Displays SNMP engine parameters	Common	*page 99*
snmp-server	Displays SNMP engine parameters	Common	*page 100*
spanning-tree	Displays the spanning tree information	Common	*page 102*
static-channel-group	Displays static channel group membership information	Common	*page 104*
terminal	Displays terminal configuration parameters	Common	*page 105*
timezone	Displays the timezone	Common	*page 106*
traffic-shape	Displays traffic shaping configuration	Common	*page 107*
users	Displays information about terminal lines	Common	*page 108*
version	Displays software and hardware version information	Common	*page 109*
wireless	Displays wireless configuration commands	Common	*page 110*
wlan-acl	Displays WLAN ACL information	Common	*page 125*
access-list	Displays the access list *Internet Protocol* (IP) configuration	Privilege/Global Config	*page 126*
aclstats	Displays ACL statistics	Privilege/Global Config	*page 127*
alarm-log	Displays all the alarms currently in the system	Privilege/Global Config	*page 128*
boot	Displays the boot configuration	Privilege/Global Config	*page 129*
clock	Displays the system clock	Privilege/Global Config	*page 130*
debugging	Displays the current debugging settings	Privilege/Global Config	*page 131*
dhcp	Displays DHCP server configurations	Privilege/Global Config	*page 132*
file	Displays filesystem information	Privilege/Global Config	*page 133*

Display Parameters	Description	Mode	Example
ftp	Displays the FTP server configuration	Privilege/Global Config	*page 134*
password-encryption	Displays password encryption data	Privilege/Global Config	*page 135*
running-config	Displays the current operating configuration	Privilege/Global Config	*page 136*
securitymgr	Displays debug information for ACL, VPN and NAT	Privilege/Global Config	*page 139*
sessions	Displays currently open and active connections	Privilege/Global Config	*page 140*
startup-config	Displays the content of the startup configuration	Privilege/Global Config	*page 141*
upgrade-status	Displays the status of the last image upgrade	Privilege/Global Config	*page 143*
mac-name	Displays the configured MAC names for this device	Privilege/Global Config	*page 144*
access-list	Displays the access list information	Privilege/Global Config	*page 126*
aclstats	Displays the ACL statistics for a particular WLAN	Privilege/Global Config	*page 127*
alarm-log	Displays the alarm log on the device	Privilege	*page 128*
firewall	Displays wireless firewall	Common	*page 145*
role	Configures role parameters	Common	*page 146*

autoinstall

Common to all modes

Displays the autoinstall configuration information.

Supported in the following platforms:

- Mobility RFS4000 Controller
- Mobility RFS6000 Controller
- Mobility RFS7000 Controller

Syntax

```
show autoinstall status
```

Parameters

status	Displays status of autoinstall

Syntax

```
RFController>show autoinstall
RFController>feature  enabled   URL
config    yes    --not-set--
cluster cfg yes    --not-set--
image    yes    --not-set--
expected image version --not-set--

RFController>
```

banner

Common to all modes

Displays the message of the day string. This string can be used to alert the user to specific information that might be of interest.

Supported in the following platforms:

- Mobility RFS4000 Controller
- Mobility RFS6000 Controller
- Mobility RFS7000 Controller

Syntax

```
show banner motd
```

Parameters

motd	Displays the *Message of the Day* banner

Example

```
RFController>show banner motd
Welcome to CLI
RFController>
```

commands

Common to all modes

Displays the available commands for the current mode.

Supported in the following platforms:

- Mobility RFS4000 Controller
- Mobility RFS6000 Controller
- Mobility RFS7000 Controller

Syntax

```
RFController>show commands
```

Parameters

None

Example

```
RFController#show commands
 acknowledge alarm-log (all|<1-65535>)
 acknowledge alarm-log (all|<1-65535>)
 archive tar /create (FILE|URL) .FILE
 archive tar /create (FILE|URL) .FILE
 archive tar /table (FILE|URL)
 archive tar /table (FILE|URL)
 archive tar /xtract (FILE|URL) DIR
 archive tar /xtract (FILE|URL) DIR
 cd (DIR|)
 cd (DIR|)
 change-passwd
 clear aclstats
 clear alarm-log (new|all|acknowledged|<1-65535>)
 clear alarm-log (new|all|acknowledged|<1-65535>)
 clear alarm-log (new|all|acknowledged|<1-65535>)
 clear alarm-log (new|all|acknowledged|<1-65535>)
 clear arp-cache
 clear crypto ipsec sa (A.B.C.D |)
 clear crypto ipsec sa (A.B.C.D |)
 clear crypto isakmp sa ( A.B.C.D |)
 clear crypto isakmp sa ( A.B.C.D |)
 clear ip dhcp binding (*|A.B.C.D)
.................................................(contd)
RFController#
```

crypto

Common to all modes

Displays the encryption mode information.

Supported in the following platforms:

- Mobility RFS4000 Controller
- Mobility RFS6000 Controller
- Mobility RFS7000 Controller

Syntax

```
show crypto[ipsec|isakmp|key|map|pki]
show crypto ipsec[sa|
security-association|transformset]
show crypto isakmp[policy <1-10000>|sa]
show crypto keymy pubkey rsa
show crypto map[interface <interface-name>|tag <tag-name>]
show crypto pki[request <trustpoint-name>|trustpoints]
```

Parameters

ipsec [sa|securityassociation |transformset]	Displays the IPSEC policy
	• sa – IPSec security association
	• security-association lifetime – Security association
	  • lifetime – Defines the lifetime
	• transformset <name> – Transformset
	  • <name> – Defines the transform set name or all transform sets

isakmp [policy <1-10000>|sa]	Displays ISAKMP policies • policy <1-10000> – Displays the priority of all the isakmp policies • sa – All crypto ISAKMP security associations
key mypubkey rsa	Displays authentication key management • mypubkey rsa – Shows the public keys associated with the controller • rsa – Displays the RSA public keys
map [interface|tag]	Displays crypto maps • interface <interface-name> – Sets crypto maps for an interface • tag <tag-name> – Sets crypto maps with a given tag
pki [request|trustpoints]	Displays Public Key Infrastructure (PKI) commands • request <trustpoint-name> – Displays the certificate requests • trustpoints – Displays the trustpoints and their configuration

Usage Guidelines

The security engine periodically updates the IPSec and Isakamp statistics (every 60 seconds)

Example

```
RFController(config)#show crypto pki request tptest
-----BEGIN CERTIFICATE REQUEST-----
MIIB2zCCAUQCAQAwaDELMAkGA1UEBhMCaW4xEjAQBgNVBAgTCWthcm5hdGFrYTES
MBAGA1UEBxMJYmFuZ2Fsb3JlMQ8wDQYDVQQKEwZzeW1ib2wxDDAKBgNVBAsTA3dp
ZDESMBAGA1UEAxMJdGVzdC1jZXJ0MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKB
gQC3qisZdTn7rKzv5TrGtKt7fwMwaYpgehyl52I4fDLZYY/WTTTJFyKwW6s+Pq2R
mM9oiqX8mCZeSEIJIATpAVT2M5Ukb4Br9YQDcWHs84oXRJxKPeZ3WscBld2soPvK
ui1LoizZH9iqawmkXED1TFMBbDWiOcfnqQKn8Tddeax/JQIDAQABoDMwMQYJKoZI
hvcNAQkOMSQwIjALBgNVHQ8EBAMCBLAwEwYDVR0lBAwwCgYIKwYBBQUHAwEwDQYJ
KoZIhvcNAQEEBQADgYEAoJMylm3aaY1CnkOO5TbxB+qL4F4MKL6+o/m0yRPqy/2S
gkk/OwxHvc3TbA9WjbKkFWIDyqU7X0d+c8f9KogwxDwWHll2IBiTCtBAq6hpgKOv
Um9GFvMFps9XVkKtYttN3fer9tA+6xY9CKlr12mNGOYFHyVjMc3Pic0ODFiPHAU=
-----END CERTIFICATE REQUEST-----

RFController(config)#show crypto pki trustpoints

Trustpoint :default-trustpoint
------------------------------------------------
 Server certificate configured
  Subject Name:
   Common Name:     Brocade
  Issuer Name:
   Common Name:     Brocade
 Valid From:  Sep 13 16:14:49 2010 GMT
 Valid Until: Sep 13 16:14:49 2010 GMT

Trustpoint :tptest
------------------------------------------------
 CA certificate configured
  Subject Name:
   Common Name:     monarch
   Organizational Unit: wid
   Organization:    Brocade
   Location:      bangalore
   State:        karnataka
   Country:       in
   email:        testuser@domain.com
  Issuer Name:
   Common Name:     monarch
   Organizational Unit: wid
   Organization:    Brocade
   Location:      bangalore
   State:        karnataka
   Country:       in
   email:        testuser@domain.com
 Valid From:  Sep 11 05:48:52 2010 GMT
 Valid Until: Sep 11 05:48:52 2010 GMT
```

environment

Common to all modes

Displays the environmental information such as fan speed, ambient temperature inside the controller and CPU temperature.

Supported in the following platforms:

- Mobility RFS4000 Controller
- Mobility RFS6000 Controller
- Mobility RFS7000 Controller

Syntax

```
show environment
```

Parameters

None

Example

```
RFController>show environment
  upwind of CPU temperature : 30.0 C
  CPU die temperature : 49.0 C
  left side temperature : 29.0 C
  by FPGA temperature : 28.0 C
  front right temperature : 26.0 C
  front left temperature : 26.0 C
  fan 1 fan     : 6480 rpm
  fan 2 fan     : 6600 rpm
  fan 3 fan     : 6420 rpm


RFController>
```

history

Common to all modes

Displays the command history

Supported in the following platforms:

- Mobility RFS4000 Controller
- Mobility RFS6000 Controller
- Mobility RFS7000 Controller

Syntax

```
show history
```

Parameters

None

Example

```
RFController>show history
  1 admin
  2 enable
  3 con ter
  4 exit
  5 show autoinstall
  6 con ter
  7 show autoinstall
  8 show banner
  9 show banner motd
 10 show command
 11 show crypto
 12 show environment
 13 show history

RFController>
```

interfaces

Common to all modes

Displays the status of the different controller interfaces

Supported in the following platforms:

- Mobility RFS4000 Controller
- Mobility RFS6000 Controller
- Mobility RFS7000 Controller

Syntax

```
show interfaces [WORD|ge|me1|sa|controllerport|vlan]
```

Parameters

show interfaces [WORD|ge|me1|sa| controllerport|vlan]	Displays the interface name • WORD– Displays interface name • ge – Displays Gigabit Ethernet interface information • me1 – Displays fast ethernet information • sa – Displays Static Aggregate information • controllerport – Displays native VLAN(s) and allowed VLAN information on controller ports • vlan[WORD|ge|me1| sa|vlan <1-4094> – Displays VLAN interface details

Usage Guidelines

Use the `show interface` command to display the administrative and operational status of all the interfaces or a specified interface

Example

```
RFController#show interfaces ge 3
Interface ge3
 Hardware Type Ethernet, Interface Mode Layer 2, address is 00-a0-f8-65-ea-8e
 index=2001, metric=1, mtu=1500, (HAL-IF) <UP,BROADCAST,MULTICAST>
 Speed: Admin Auto, Operational Unknown, Maximum 1G
 Duplex: Admin Auto, Operational Unknown
 Active Medium: Unknown
 Controllerport Settings: access, access-vlan: 1
    Input packets 0, bytes 0, dropped 0,
    Received 0 broadcasts, 0 multicasts
    Input errors 0, runts 0, giants 0,
    CRC 0, frame 0, fragment 0, jabber 0
    Output packets 0, bytes 0, dropped 0
    Sent 0 broadcasts, 0 multicasts
    Output errors 0, collisions 0, late collisions 0,
    excessive collisions 0

RFController#show interfaces wan
Interface wan
Hardware Type PPP, Interface Mode Layer 3
index=8, metric=1, mtu=1500, (PAL-IF)  <UP,POINTOPOINT,RUNNING,NOARP,MULTICAST
>
inet 166.129.246.245/32 pointopoint 10.64.64.64
input packets 0, bytes 0, dropped 0, multicast packets 0
```

```
input errors 0, length 0, overrun 0, CRC 0, frame 0, fifo 0, missed 0
output packets 184, bytes 17618, dropped 0
output errors 0, aborted 0, carrier 0, fifo 0, heartbeat 0, window 0
collisions 0
index=8, metric=1, mtu=1500, (PAL-IF)  <UP,POINTOPOINT,RUNNING,NOARP,MULTICAST
>
inet 166.129.246.245/32 pointopoint 10.64.64.64
input packets 0, bytes 0, dropped 0, multicast packets 0
input errors 0, length 0, overrun 0, CRC 0, frame 0, fifo 0, missed 0
output packets 184, bytes 17618, dropped 0
output errors 0, aborted 0, carrier 0, fifo 0, heartbeat 0, window 0
collisions 0

RFController(config)#show interfaces controllerport vlan1
Interface vlan1
 Controllerport Settings: Mode: Access, Access Vlan: 0
```

ip

Common to all modes

Displays Internet Protocol (IP) related information

Supported in the following platforms:

- Mobility RFS4000 Controller
- Mobility RFS6000 Controller
- Mobility RFS7000 Controller

Syntax

```
show ip [access-group|arp|ddns|dhcp|
dhcp-vendor-options|domain-name|dos|http|igmp|interface|
name-server|nat|route|routing|ssh|telnet]
show ip access-group [<interface-name>|all|ge|me1|role|sa|
vlan <1-4094>]
show ip arp
show ip ddnsbinding
show ip dhcp[binding|class|pool|sharednetwork]
show ip dhcp-vendor-options
show ip domain-name
show ip dos [config|stats]
show ip http [secure-server|server]
show ip igmp snooping [mrouter|querier|vlan]
show ip interface [<interface-name>|brief|ge|me1|sa|vlan]
show ip name-server
show ip nat [interfaces|translations]
show ip nat translations [inside|outside|verbose]
show ip nat translations inside [source|destination]
show ip nat translations outside [source|destination]
show ip route [<IP>|<IP-prefix-len>|detail]
show ip routing
show ip ssh
show ip telnet
```

Parameters

access-group [<interface-name> |all|ge|me1|role|sa|> |vlan <1-4094>]	Displays the ACLs attached to an interface • <interface-name> – Enter the name of the interface to which the ACL is associated. access-group lists the details of the ACLs configured on the particular Layer 3 or Layer 2 interface. • vlan <1-4094> – Enter the name of the VLAN interface to which the ACL is associated • all – Display ACLs attached on all interfaces • ge <1-4> – Gigabit Ethernet interface • me1– FastEthernet interface • role <role-name> – Specify role name • sa <1-4> – Static Aggregate interface
arp	Displays existing entries in the *Address Resolution Protocol* (ARP) table
ddns binding	Displays the DDNS configuration • binding – DNS address bindings
dhcp [binding|class|pool |sharednetwork]	Displays the DHCP server configuration • binding manual – DNS address bindings • manual – Static DHCP Address Bindings class – Configures the DHCP server class • pool – DHCP pool designation • sharednetwork – Shared network information
dhcp-vendor-options	DHCP Option 43 parameters received from DHCP server
domain-name	Displays domain name information
dos [config|stats]	Denial of Service configuration • config – Displays ip dos configuration • stats – Displays ip dos stats
http [secure-server|server]	*Hyper Text Transfer Protocol* (HTTP) • secure-server – Secure HTTP server • server – HTTP server
interface [<interface-name>|brief|ge |me1|sa| vlan]	Use the show ip interface command to display the administrative and operational status of all Layer-3 interfaces or a specified Layer-3 interface. • <interface-name> – Interface name • brief – Brief summary of the IP status and its configuration • vlan <1-4094> – VLAN Interface • ge <1-4>– GigabitEthernet interface • me1– FastEthernet interface • sa <1-4> – Static Aggregate interface

igmp snooping [mrouter|querier|vlan]	Displays Internet Group Management Protocol
	• snooping – IGMP Snooping
	  • mrouter – Displays Multicast Router
	  • querier – Configure IGMP querier
	  • vlan [<1-4094>|<vlan-list>] – Identify the vlan to use

name-server	Displays static and dynamic name-server entries

nat [interfaces|translations]	Displays Network Address Translation
	• interfaces – Displays NAT Configuration on interfaces
	• translations [inside|outside|verbose] – Displays NAT translations
	  • inside [source|destination]– Inside
	  • outside [source|destination] – Outside
	  • source – Displays Source
	  • destination – Displays Destination
	  • verbose – Displays NAT Translations in real-time

route [<IP>|<IP/Mask> |detail]	Display IP routing table entries • <IP> – Network in the IP routing table • <IP/Mask> – Number of valid bits in the network prefix IP prefix <network>/<length>, e.g., 35.0.0.0/8 • detail – Displays the IP routing table in detail
routing	IP routing status
ssh	Secured Shell (SSH) server
telnet	Telnet server

Usage Guidelines

1. The interface and VLAN status is displayed as UP regardless of a disconnection. In such a case, shutdown the VLAN.

   a. Check the status of an interface and VLAN using:

   ```
   RFController(config)#show ip interface brief
   Interface       IP-Address      Status        Protocol
   vlan1         157.235.208.69(DHCP) up        up
   vlan3         unassigned       up          up
   RFController(config)#
   ```

   If the status of the VLAN is UP, shutdown the VLAN associated with eth1 using:

   ```
   RFController(config-if)#show ip interface vlan 3 brief
   Interface       IP-Address      Status        Protocol
   vlan3         unassigned       up          up
   RFController(config-if)#shutdown
   ```

   b. Check the status. Note that the VLAN has now been disassociated and the status is DOWN.

   ```
   RFController(config)#show ip interface brief
   Interface       IP-Address       Status        Protocol
   vlan1        157.235.208.69(DHCP)  up          up
   vlan3         unassigned       administratively down down
   RFController(config)#
   ```

2. The above example could also occur when a DHCP interface is disconnected. DHCP is not effected though, because it runs on a virtual interface and not on a physical interface. In this case, it is the physical interface that is disconnected not the virtual interface. When the ethernet interface comes back up, it will restart the DHCP client on any virtual interfaces (SVIs) of which the physical interface is a member port. This ensures if the interface was disconnected and reconnected to a different interface, it obtains a new IP address, route, name server, domain name etc.

Example

```
RFController(config)#show ip access-group ge 3
Interface ge3
 Inbound IP Access List :

RFController(config)#show ip access-group vlan 1
Interface vlan1
 Inbound IP Access List :

RFController#show ip dhcp binding
IP       MAC/Client-Id   Type    Expiry Time
--       -------------   ----    -----------

RFController(config)#show ip dhcp class
!
ip dhcp class TestClass2
 option user-class MC900
!
ip dhcp class ImportantClass
!
ip dhcp class ClassNameTest
 option user-class UserClassTest
!
ip dhcp class TestDHCPclass
!
ip dhcp class Add-DHCP-class1
!
ip dhcp class MonarchDHCPclas
 option user-class MC9000
!
ip dhcp class RFControllerDHCPclass
 option user-class MC800
RFController(config)#

RFController#show ip dhcp pool
!
ip dhcp pool pl
!
ip dhcp pool pool1
 domain-name test.com
 bootfile 123
 network 10.10.10.0/24
 address range 10.10.10.2 10.10.10.30
!
ip dhcp pool poo110
 next-server 1.1.1.1
 netbios-node-type b-node

RFController#show ip dhcp-vendor-options
Server Info:
Firmware Image File:
Config File:
Cluster Config File:

RFController#show ip domain-name
 IP domain-lookup : Enable
 Domain Name  : brocade.com

RFController#show ip http server
```

```
HTTP server: Running
Config status: Enabled

RFController#show ip http secure-server
HTTP secure server: Running
Config status: Enabled
Trustpoint: default-trustpoint

RFController#show ip interface brief
Interface        IP-Address/Mask  Status  Protocol
me1              10.1.1.100/24      up      down
vlan1            192.168.1.1/24     up      up
vlan11           192.168.11.1/24    up      up
vlan2            64.171.249.249/24  up      up
wan              166.129.246.245/32 up      up
RFController#

RFController#show ip interface vlan 1 brief
Interface   IP-Address    Status   Protocol
vlan1     157.235.208.233  (DHCP)up  up

RFController#show ip name-server
157.235.3.195      dynamic
157.235.3.196      dynamic

RFController#show ip routing
IP routing is on

RFController(config)#show ip route detail
Codes: K - kernel/icmp, C - connected, S - static, D - DHCP
    > - Active route, - Next-hop in FIB, p - stale info

S    1.1.0.0/16 [1/0] via 1.1.1.1 inactive
S    1.1.1.0/24 [1/0] via 1.1.1.2 inactive
S    10.0.0.0/8 [1/0] via 10.10.10.10 inactive
S    157.235.208.0/24 [1/0] via 157.235.208.246 inactive

RFController#show ip ssh
SSH server: enabled
Status: running
Keypair name: default_ssh_rsa_key
Port: 22

RFController#show ip telnet
Telnet server: enabled
Status: running
Port: 23
```

ldap

Common to all modes

Displays LDAP information

Supported in the following platforms:

- Mobility RFS4000 Controller
- Mobility RFS6000 Controller
- Mobility RFS7000 Controller

Syntax

```
show ldap configuration [primary|secondary]
```

Parameters

ldap configuration [primary|secondary]	Displays LDAP information.
	• Configuration [primary|secondary] – Sets the LDAP configuration server parameters
	  • primary – Defines the Primary LDAP server
	  • secondary – Defines the Secondary LDAP server

Example

```
RFController(config-radsrv)#show ldap configuration
LDAP Server Config Details

Primary LDAP Server configuration

    IP Address       : 10.10.10.1
    Port          : 369
    Login         :
(sAMAccountName=%{Stripped-User-Name:-%{User-Name}})
    Bind DN        : cn=kumar,ou=brocade,dc=activedirectory,dc=com
    Base DN        : ou=brocade,dc=activedirectory,dc=com
    Password        : 0 brocade@123
    Password Attribute   : UserPassword
    Group Name       : cn
    Group Membership Filter: (&(objectClass=group)(member=%{Ldap-UserDn}))
    Group Member Attr   : radiusGroupName
    Net timeout      : 1 second(s)

Secondary LDAP

    IP Address       : 10.10.10.5
    Port          : 369
    Login         :
(sAMAccountName=%{Stripped-User-Name:-%{User-Name}})
    Bind DN        : cn=kumar,ou=brocade,dc=activedirectory,dc=com
    Base DN        : ou=brocade,dc=activedirectory,dc=com
    Password        : 0 brocade@123
    Password Attribute   : UserPassword
    Group Name       : cn
    Group Membership Filter: (&(objectClass=group)(member=%{Ldap-UserDn}))
    Group Member Attr   : radiusGroupName
    Net timeout      : 1 second(s)
```

licenses

Common to all modes

Displays the different licenses installed on the controller

Supported in the following platforms:

- Mobility RFS4000 Controller
- Mobility RFS6000 Controller
- Mobility RFS7000 Controller

Syntax

```
show licenses
```

Parameters

None

Example

```
RFController(config)#show licenses
feature usage license string       license value  usage
AP       2FFD7fE9 CD016155 14A92C70 48     1
```

logging

Common to all modes

Displays logging status and other information

Supported in the following platforms:

- Mobility RFS4000 Controller
- Mobility RFS6000 Controller
- Mobility RFS7000 Controller

Syntax

```
show logging
```

Parameters

None

Example

```
RFController(config)#show logging

Logging module: enabled
  Aggregation time: disabled
  Console logging: level debugging
  Buffered logging: level informational
  Syslog logging: level debugging
    Facility: local7
    Logging to: 157.235.203.37
    Logging to: 10.0.0.2

Log Buffer (6520 bytes):

Sep 14 19:11:59 2010: %DAEMON-6-INFO: radiusd[4643]: Ready to process
requests.

Sep 14 19:11:58 2010: %PM-5-PROCSTOP: Process "radiusd" has been stopped

Sep 14 18:51:14 2010: %CC-5-RADIOADOPTED: 11a radio on AP 00-A0-F8-BF-8A-A2
adopted

Sep 14 18:51:14 2010: %CC-5-RADIOADOPTED: 11bg radio on AP 00-A0-F8-BF-8A-A2
adopted
```

mac

Common to all modes

Shows all MAC information with respect to groups and access lists

Supported in the following platforms:

- Mobility RFS4000 Controller
- Mobility RFS6000 Controller
- Mobility RFS7000 Controller

Syntax

```
show mac [access-list|access-group]
show mac access-group [<interface>|all|ge <1-4>|
me1|sa <1-4>|vlan <1-4094>]
```

Parameters

mac [access-list access-group]	Displays MAC information
	• access-list – Displays existing MAC access lists
	• access-group [<Interface>|all|ge <1-4>| me1|sa <1-4>|vlan<1-4094>] – Displays MACs access control lists (ACLs) attached the specified interface where:
	  • <interface> – Name of the interface
	  • all interfaces
	  • ge <1-4> – The specified Gigabit interface
	  • me1 – The fast ethernet interface
	  • sa <1-4> – The specified Static Aggregate interface
	  • vlan <1-4094> – VLAN
	  • <1-4094> – Displays VID

Example

```
RFController(config)#show mac access-list
RFController(config)#show mac access-group all
```

mac-address-table

Common to all modes

Displays the MAC address table entries

Supported in the following platforms:

- Mobility RFS4000 Controller
- Mobility RFS6000 Controller
- Mobility RFS7000 Controller

Syntax

```
show mac-address-table
```

Parameters

None

Example

```
RFController(config)#show mac-address-table

Bridge    VLAN Port     Mac      Fwd
----------- ---- ------------ -------------- ---
1      10  ge1     00a0.f865.ea8f 1
1      10  ge1     0015.7038.0653 1
1      10  ge1     0015.7014.fec4 1
1      10  ge1     0015.7041.9f7f 1

RFController(config)
```

management

Common to all modes

Displays the L3 management interface name

Supported in the following platforms:

- Mobility RFS4000 Controller
- Mobility RFS6000 Controller
- Mobility RFS7000 Controller

Syntax

```
show management
```

Parameters

None

Example

```
RFController>show management
Mgmt Interface: vlan1
Management access permitted via any vlan interface
RFController>
```

mobility

Common to all modes

Displays the mobility parameters

Supported in the following platforms:

- Mobility RFS4000 Controller
- Mobility RFS6000 Controller
- Mobility RFS7000 Controller

Syntax

```
show mobility [event-log|forwarding|global|
wireless-client|peer|statistics]
show mobility event-log [wireless-client|peer]
show mobility forwarding <MAC>
show mobility wireless-client [MAC>|detail]
show mobility peer [<IP>|detail]
show mobility statistics <MAC>
```

Parameters

event-log[wireless-client|peer]	Displays mobility event logs • wireless-client – Client event logs • peer – Peer event logs
forwarding <MAC>	Displays and defines wireless clients in the forwarding plane • <MAC> – MAC address of the wireless client
global	Displays and defines global mobility parameters
wireless-client [<MAC>| detail]	wireless clients in the mobility database • <MAC> – MAC address of the wireless client • detail – Displays detailed information
peer [<IP>|detail]	Mobility peers • <IP> – IP address of Peer • detail – Displays detailed peer information
statistics <MAC>	Mobility statistics • <MAC> – MAC address of the wireless client

Example

```
RFController(config)#show mobility ?
 event-log  Event Log
 forwarding  Wireless-client information in the forwarding plane
 global    Global Mobility parameters
 wireless-client Wireless-clients in the Mobility Database
 peer     Mobility peers
 statistics  Wireless-client Statistics

RFController(config)#show mobility event-log wireless-client
Time      Event    Evt-Src-IP   CLIENT-Mac       CLIENT-IP
HS-IP      CS-IP
09/14 19:17:52 IP-UPD-CLIENT  n/a       00-0f-3d-e9-a6-54
157.235.208.134 157.235.208.16 157.235.208.16
09/14 19:17:51 ADD-CLIENT    n/a       00-0f-3d-e9-a6-54 0.0.0.0
157.235.208.16 157.235.208.16
```

```
09/14 19:17:51 DEL-CLIENT    n/a       00-0f-3d-e9-a6-54 0.0.0.0
157.235.208.16 157.235.208.16
09/14 19:17:50 ADD-CLIENT    n/a       00-0f-3d-e9-a6-54 0.0.0.0
157.235.208.16 157.235.208.16

RFController>show mobility forwarding
Mobility Forwarding-plane Information
 State: HS : Home-controller    CS : Current-controller
     !HS: Not Home-controller  !CS: Not Current-controller
Mac-Address    IP-Address   State  HS-Vlan  Tunnel
RFController>

RFController>show mobility global
Mobility Global Parameters
Admin Status           : DISABLED
Operational-Status        : DISABLED (Admin-status is DISABLED)
Local Address           : 10.10.10.2 (mgmt-vlan)
Port Number            : 58788
Max Roam Period          : 5 sec
Number of Peers          : 0 (established=0)
Number of Clients           : 0 (Home=0, Foreign=0, Delete-pend=0)
L3-Mobility enabled WLANs     : NONE
RFController>

RFController(config)#show mobility wireless-client detail
HOME CLIENT Database: Total=1
CLIENT MAC-Address: 00-0f-3d-e9-a6-54, IP-Address: 157.235.208.134,
SSID=wios_rad_test1
 Home-Controller: 157.235.208.16, Current-Controller: 157.235.208.16,
HS-VLAN=1
Foreign CLIENT Database: Total=0

RFController(config)#show mobility peer detail
Mobility Peers: Total=1, Established=0
Peer: 1.1.1.1, State: PASSIVE-CONNECTING
 Join-Sent : 0   Join-Rcvd : 0   Leave-Sent : 0   Leave-Rcvd : 0
 Rehome-Sent: 0   Rehome-Rcvd: 0   L3roam-Sent: 0   L3roam-Rcvd: 0
 Num-flaps : 0   Connect-retries: 0  Peer-Uptime: 0 days, 00:00:00

RFController(config)#show mobility statistics

CLIENT <00-0f-3d-e9-a6-54> Mob-State HS_AND_CS
-----------------------------------------------
Inter-     |Rx                    |Tx
face      |unicast  MC     BC     Error   |unicast  MC
BC     Error
wlan_port    0     0     0     0     0     0
0     0
```

ntp

Common to all modes

Displays NTP protocol information

Supported in the following platforms:

- Mobility RFS4000 Controller
- Mobility RFS6000 Controller
- Mobility RFS7000 Controller

Syntax

```
show ntp [association|status]
```

Parameters

ntp [association detail|status]	Displays the *Network Time Protocol* (NTP) configuration • association detail – Displays existing NTP associations • detail – Displays NTP association details • status – Displays NTP status

Example

```
RFController>show ntp associations
 address     ref clock    st when poll reach delay offset  disp
 * master (synced), # master (unsynced), + selected, - candidate, ~ configured
RFController>

RFController>show ntp status
Clock is synchronized, stratum 0, actual frequency is 0.0000 Hz, precision is
2**0
reference time is 00000000.00000000 (Feb 07 06:28:16 UTC 2036)
clock offset is 0.000 msec, root delay is 0.000 msec
root dispersion is 0.000 msec,
RFController>

RFController(config)#show ntp associations detail
157.235.208.105 configured, sane, valid, leap_sub, stratum 16
ref ID INIT, time 00000000.00000000 (Feb 07 06:28:16 UTC 2036)
our mode client, peer mode unspec, our poll intvl 6, peer poll intvl 10
root delay 0.00 msec, root disp 0.00, reach 000,
delay 0.00 msec, offset 0.0000 msec, dispersion 0.00
precision 2**-20,
org time 00000000.00000000 (Feb 07 06:28:16 UTC 2036)
rcv time 00000000.00000000 (Feb 07 06:28:16 UTC 2036)
xmt time c8b42a7e.6eb04252 (Sep 14 19:22:38 UTC 2010)
filtdelay = 0.00 0.00 0.00 0.00 0.00 0.00 0.00 0.00



RFController>show ntp status
Clock is synchronized, stratum 0, actual frequency is 0.0000 Hz, precision is
2^0
reference time is 00000000.00000000 (Feb 07 06:28:16 UTC 2036)
clock offset is 0.000 msec, root delay is 0.000 msec
root dispersion is 0.000 msec,
RFController>
```

port-channel

Common to all modes

Displays port-channel load-balance information

- Mobility RFS7000 Controller
- Mobility RFS4000 Controller

NOTE
This command is not supported on the Mobility RFS6000 Controller.

Syntax

```
show port-channel load-balance
```

Parameters

load-balance	Displays the existing load balancing configuration

Example

```
RFController>show port-channel load-balance
RFController>
```

power

Common to all modes

Displays the power configuration and status for the Mobility RFS6000 Controller controller

Supported in the following platforms:

- Mobility RFS4000 Controller
- Mobility RFS6000 Controller

NOTE
This command is not supported on the Mobility RFS7000 Controller.

Syntax

```
show power [configuration|status]
```

Parameters

configuration	Displays configuration of power over ethernet
status	Displays status of power over ethernet

Example

```
RFController(config)#show power configuration

Power usage trap at 80% of max power (148 of 185 Watts)

 port Priority  Power limit Enabled
 ge1 high    29.7W    yes
 ge2 high    29.7W    yes
 ge3 high    29.7W    yes
 ge4 high    29.7W    yes
 ge5 high    29.7W    yes
 ge6 high    29.7W    yes
 ge7 high    29.7W    yes
 ge8 high    29.7W    yes

 POE firmware version 01f6 build 4

RFController(config)#
```

privilege

Common to all modes

Displays the privileges of the current user

Supported in the following platforms:

- Mobility RFS4000 Controller
- Mobility RFS6000 Controller
- Mobility RFS7000 Controller

Syntax

```
show privilege
```

Parameters

None

Example

```
RFController>show privilege
Current user privilege: superuser
RFController>
```

radius

Common to all modes

Displays RADIUS status and information

Supported in the following platforms:

- Mobility RFS4000 Controller
- Mobility RFS6000 Controller
- Mobility RFS7000 Controller

Syntax

```
show radius [configuration|eap configuration|group|
nas  A.B.C.D/M|proxy|rad-user|trust-point]
```

Parameters

radius [configuration| eap configuration group| nas <IP/Mask>|proxy| rad-user|trust-point]	Displays RADIUS configuration commands • configuration – RADIUS server configuration parameters • eap configuration – Displays and defines the EAP configuration • group – Displays the RADIUS group configuration • nas <IP/Mask> – Defines a client IP address and mask • proxy – Lists proxy information • rad-user <user-name> – Displays RADIUS user information • user-name - Displays existing user name in the local RADIUS database. • trust-point – Defines the RADIUS trust-point configuration

Example

```
RFController(config)#show radius proxy
Proxy Details
_____________
Proxy retry delay : 6 seconds
Proxy retry count : 4

Proxy Realm Details
___________________
Realm  : brocade.com
    IP Address  : 10.10.10.5
    Port     : 1812
    Shared secret : 0 secret123
```

redundancy dynamic-ap-load-balance

Common to all modes

Displays the configuration for the Dynamic AP Load Balancing feature

Supported in the following platforms:

- Mobility RFS4000 Controller
- Mobility RFS6000 Controller
- Mobility RFS7000 Controller

Syntax

```
show redundancy dynamic-ap-load-balance config
```

Parameters

config	Displays configuration details for dynamic AP load balance

Example

```
RFController(config)#show redundancy dynamic-ap-load-balance config
Dynamic AP Load Balance Configuration:
 Load balance     : Enabled
 Load balance trigger : Schedule

Dynamic AP Load Balance Schedule:
 Schedule first-time  : Sun Jun 1 00:00:00 2008
 Schedule interval   : 1 day(s)

Per AP CLIENT Threshold   : 32
RFController(config)#
```

redundancy group

Common to all modes

This command displays the controller's IP address, number of active neighbors, group license, installed license, cluster AP adoption count, controller adoption count, hold time, discovery time, heartbeat interval, cluster id and controller mode.

In a cluster, this command displays the redundancy runtime and configuration of the "self-controller". Use `config` to view only configuration information and/or `runtime` parameters.

Supported in the following platforms:

- Mobility RFS4000 Controller
- Mobility RFS6000 Controller
- Mobility RFS7000 Controller

Syntax

```
show redundancy group [config|runtime]
```

Parameters

redundancy group [config | runtime]	Displays redundancy runtime and configuration details. • config – Displays configured redundancy group information • runtime – Displays runtime redundancy group information

Example

```
RFController(config)#show redundancy group

Redundancy Group Configuration Detail
Redundancy Feature         : Disabled
Redundancy group ID        : 1
Redundancy Mode          : Primary
Redundancy Interface IP      : 0.0.0.0
Number of configured peer(s)    : 0
Heartbeat-period          : 5 Seconds
Hold-period            : 15 Seconds
Discovery-period          : 30 Seconds
Handle STP             : Disabled
Controller Installed License      : 48
Controller running image version    : 4.02.0
Auto-revert-period         : 5 mins
Auto-revert Feature        : Disabled
DHCP-Server Redundancy       : Disabled

Redundancy Group Runtime Information
Redundancy Protocol Version     : 2.0
Redundancy Group License       : 0
Cluster AP Adoption Count      : Not Applicable
Controller AP Adoption Count       : Not Applicable
Redundancy State           : Disabled
Radio Portals adopted by Group    : Not Applicable
Radio Portals adopted by this Controller : Not Applicable
Rogue APs detected in this Group   : Not Applicable
Rogue APs detected by this Controller  : Not Applicable
Clients associated in this Group     : Not Applicable
Clients associated in this Controller    : Not Applicable
```

```
Selfhealing RPs in this Group    : Not Applicable
Selfhealing APs in this Controller    : Not Applicable
Group maximum AP adoption capacity  : Not Applicable
Controller Adoption capacity       : Not Applicable
Established Peer(s) Count      : Not Applicable
Redundancy Group Connectivity status : Not Applicable
DHCP Server in group         : Not Applicable

RFController(config)#


RFController(config)#show redundancy group config

Redundancy Group Configuration Detail
Redundancy Feature         : Disabled
Redundancy group ID        : 1
Redundancy Mode          : Primary
Redundancy Interface IP      : 0.0.0.0
Number of configured peer(s)    : 0
Heartbeat-period          : 5 Seconds
Hold-period            : 15 Seconds
Discovery-period          : 30 Seconds
Handle STP             : Disabled
Controller Installed License      : 48
Controller running image version    : 4.02.0
Auto-revert-period         : 5 mins
Auto-revert Feature        : Disabled
DHCP-Server Redundancy       : Disabled

RFController(config)#

RFController(config)#show redundancy group runtime

Redundancy Group Runtime Information
Redundancy Protocol Version     : 2.0
Redundancy Group License       : 0
Cluster AP Adoption Count      : Not Applicable
Controller AP Adoption Count       : Not Applicable
Redundancy State           : Disabled
Radio Portals adopted by Group    : Not Applicable
Radio Portals adopted by this Controller : Not Applicable
Rogue APs detected in this Group   : Not Applicable
Rogue APs detected by this Controller  : Not Applicable
Clients associated in this Group     : Not Applicable
Clients associated in this Controller    : Not Applicable
Selfhealing RPs in this Group    : Not Applicable
Selfhealing APs in this Controller    : Not Applicable
Group maximum AP adoption capacity  : Not Applicable
Controller Adoption capacity       : Not Applicable
Established Peer(s) Count      : Not Applicable
Redundancy Group Connectivity status : Not Applicable
DHCP Server in group         : Not Applicable

RFController(config)#
```

redundancy history

Common to all modes

Displays the controller state transition history

Supported in the following platforms:

- Mobility RFS4000 Controller
- Mobility RFS6000 Controller
- Mobility RFS7000 Controller

Syntax

```
show redundancy history
```

Parameters

None

Example

```
RFController>show redundancy history
State Transition History

Time         Event Triggered     state
-------------------------------------------------------
Sat Oct 06 12:07:55  Redundancy Enabled   Startup
Sat Oct 06 12.07.56   Startup Done         Discovery
Sat Oct 06 12:08:26  Discovery Done     Active
Sat Oct 06 22:10:10  Redundancy Disabled   Startup

RFController>show
```

redundancy members

Common to all modes

Displays the member controllers in the cluster. The user can provide the `IP address` of the controller in cluster whose information alone is needed.

Supported in the following platforms:

- Mobility RFS4000 Controller
- Mobility RFS6000 Controller
- Mobility RFS7000 Controller

Syntax

```
show redundancy members [<IP>|brief]
```

Parameters

redundancy members [<IP>|brief]	Displays member controllers in the cluster • <IP>– Displays the IP addresses of member controllers • brief – Displays members in brief

Example

```
RFController(config)#show redundancy members brief

Member ID (Self)       : 10.10.10.10
Member State          : Not Applicable

Member ID            : 10.10.10.1
Member State          : Peer Configured
```

rtls

Common to all modes

Displays the Real Time Locating System status and information

Supported in the following platforms:

- Mobility RFS4000 Controller
- Mobility RFS6000 Controller
- Mobility RFS7000 Controller

Syntax

```
show rtls [aeroscout|espi|filter|ekahau|
reference-tags|rfid|site|sole|tags|zone]
```

Parameters

rtls [aeroscout|espi|filter|ekahau|reference-tags|rfid|site|sole|tags|zone]	Displays the Real Time Locating System status and information.
	• aeroscout – Displays aeroscout configurations
	• espi [adapter|ecspecs|subscriber|tags] – Displays ESPI configuration
	  • adapter [active|ale-tcp] – Displays Adapter Configuration
	  • active – Displays adapters that are currently active
	  • ale-tcp – Displays ale-tcp adapter
	  • ecspecs [<SPECNAME>|active|define|detail|requested] – Displays ecsspecs configuration
	  • <SPECNAME> – Displays name of Ec Specs
	  • active detail – Displays detailed active ECSpecs status
	  • defined detail – Displays defined active ECSpecs status in detail
	  • detail – Show detailed ECSpecs status
	  • requested detail – Displays requested detailed ECSpecs status
	  • subscriber – Displays info for given subscriber's IP
	  • tags subscriber – Displays tags for given subscriber's IP
	• filter – Displays RFID tag filters
	• ekahau – Displays ekahau configurations
	• reference-tags – Displays reference tag configurations
	• rfid – Displays RFID configuration
	• site – Displays site configurations
	• sole – Displays SOLE configurations
	• zone <1-48> – Displays zone configuration

rtls tags [<tag-id>|aeroscout|all|ekahau|g2|wireless-client||rfid|uri|zone|]	Displays Tags/Assets (passive, active, wi-fi, uwb) Information • <tag-id> – Displays detailed tag information for specific tag ID • aeroscout – Displays located aeroscout tags • all – Displays all tags • ekahau – Displays located ekahau tags • g2 – Displays located g2 tags • wireless-client – Displays located wireless clients • rfid - Displays located RFID gen2 tags • uri <URI> – Displays RFID tags for given notification URI • zone <1-48> – Display zone configuration
zone [<1-48>|detail]	Displays logical reader statistics • <1-48> – Display zone configuration • detail – Displays zone details

Example

```
RFController(config)#show rtls ?
 aeroscout    Aeroscout configurations
 espi      ESPI Configuration
 filter    RFID Tag Filters
 ekahau    Ekahau configurations
 reference-tags Reference tag Configurations
 rfid      RFID Configuration
 site      Site configurations
 sole      SOLE configurations
                 Information
```

```
 zone      Show logical reader statistics
RFController(config)#show rtls
```

smtp-notification

Common to all modes

Displays the set smtp-notification parameters

Supported in the following platforms:

- Mobility RFS4000 Controller
- Mobility RFS6000 Controller
- Mobility RFS7000 Controller

Syntax

```
show smtp-notification traps
```

Parameters

traps	Displays trap enable flags

Example

```
RFController(config)#show smtp-notification traps
-----------------------------------------------------------------Gl
obal enable flag for Trap SMTP-Notification      Disabled
-----------------------------------------------------------------En
able flag status for Individual Trap SMTP-Notification
-----------------------------------------------------------------M
odule Type        Trap Type         Enabled?[Y/N]
-----------------------------------------------------------------s
nmp            coldstart              N
snmp              linkdown               N
snmp              linkup                 N
snmp              authenticationFail     N
nsm               dhcpIPChanged          N
diagnostics       tempHigh               N
diagnostics       tempOver               N
diagnostics       fanSpeedLow            N
diagnostics       cpuLoad1Min            N
diagnostics       cpuLoad5Min            N
diagnostics       cpuLoad15Min           N
diagnostics       usedKernelBuffer       N
diagnostics       ramFree                N
diagnostics       processMemoryUsage     N
diagnostics       packetBuffers          N
diagnostics       ipRouteCache           N
diagnostics       fileDescriptors        N
redundancy        memberUp               N
redundancy        memberDown             N
redundancy        memberMisConfigured         N
redundancy        adoptionExceeded            N
redundancy        grpAuthLevelChanged         N
redundancy        resourceUp                  N
```

```
redundancy        resourceDown                N
misc           lowFsSpace                     N
misc           processMaxRestartsReached      N
misc           savedConfigModified            N
misc           serverCertExpired              N
misc           caCertExpired                  N
misc           periodicHeartbeat              N
misc           controllerEvent                    N
wireless station     associated               N
wireless station     disassociated             N
wireless station     deniedAssociationOnCapability     N
wireless station     deniedAssociationOnShortPream     N
wireless station     deniedAssociationOnSpectrum       N
wireless station     deniedAssociationOnErr            N
wireless station     deniedAssociationOnSSID           N
wireless station     deniedAssociationOnRates          N
wireless station     deniedAssociationOnInvalidWPAWPA2IE    N
wireless station     deniedAssociationAsPortCapacityReached N
wireless station     tkipCounterMeasures           N
wireless station     deniedAuthentication          N
wireless station     radiusAuthFailed              N
wireless station     vlanChanged                   N
wireless radio      adopted                        N
wireless radio      unadopted                      N
wireless radio      detectedRadar                  N
wireless ap-detection  externalAPDetected          N
wireless ap-detection  externalAPRemoved           N
wireless self-healing  activated                   N
wireless ids       muExcessiveEvents               N
wireless ids       radioExcessiveEvents            N
.....................................................
.....................................................
RFController(config)#
```

snmp

Common to all modes

Displays SNMP user information

Supported in the following platforms:

- Mobility RFS4000 Controller
- Mobility RFS6000 Controller
- Mobility RFS7000 Controller

Syntax

```
show snmp user [snmpmanager|snmpoperator|snmptrap]
```

Parameters

snmp user [snmpmanager| snmpoperator|snmptrap	Displays SNMP user information • snmpmanager – Shows SNMP manager information • snmpoperator – Shows SNMP operator information • snmptrap – Shows SNMP trap information

Example

```
RFController>show snmp user snmpmanager
userName   access  engineId          Authentication Encryption
snmpmanager  rw    800001848067458b6bd7157745 MD5       DES
RFController>

RFController>show snmp user snmpoperator
userName   access  engineId          Authentication Encryption
snmpoperator ro    800001848067458b6bd7157745 MD5       DES
RFController>

RFController>show snmp user snmptrap
userName   access  engineId          Authentication Encryption
snmptrap   rw    800001848067458b6bd7157745 MD5       DES
RFController>
```

snmp-server

Common to all modes

Displays SNMP server information

Supported in the following platforms:

- Mobility RFS4000 Controller
- Mobility RFS6000 Controller
- Mobility RFS7000 Controller

Syntax

```
show snmp-server traps wireless-statistics[mesh|wireless-client|
radio|wireless-controller|wlan]
```

Parameters

traps wireless-statistics [mesh| wireless-client| radio| wireless-controller|wlan]	Displays existing wireless-stats rate trap enabled flags • mesh – Displays existing mesh rate traps • wireless-client – Displays existing wireless client rate traps • radio – Displays existing radio rate traps • wireless-controller – Displays existing wireless controller rate traps • wlan – Displays existing WLAN rate traps

Example

```
RFController>show snmp-server traps
-----------------------------------------------------------------
Global enable flag for Traps                  N
-----------------------------------------------------------------
Enable flag status for Individual Traps
-----------------------------------------------------------------
Module Type        Trap Type         Enabled?[Y/N]
-----------------------------------------------------------------
snmp              coldstart               N
snmp              linkdown                N
snmp              linkup                  N
snmp              authenticationFail      N
nsm               dhcpIPChanged           N
redundancy        memberUp                N
redundancy        memberDown              N
redundancy        memberMisConfigured     N
redundancy        adoptionExceeded        N
redundancy           grpAuthLevelChanged          N
misc                 lowFsSpace                   N
misc                 processMaxRestartsReached    N
wireless station     associated                   N
wireless station     disassociated                N
wireless station     deniedAssociationOnCapability     N
wireless station     deniedAssociationOnShortPream     N
wireless station     deniedAssociationOnSpectrum       N
wireless station     deniedAssociationOnErr            N
wireless station     deniedAssociationOnSSID           N
wireless station     deniedAssociationOnRates          N
wireless station     deniedAssociationOnInvalidWPAWPA2IE  N
wireless station     deniedAssociationAsPortCapacityReached N
```

```
wireless station     tkipCounterMeasures          N
wireless station     deniedAuthentication         N
wireless station     radiusAuthFailed             N
wireless radio       adopted                      N
wireless radio       unadopted                    N
wireless radio       detectedRadar                N
wireless ap-detection  externalAPDetected         N
wireless self-healing  activated                  N
wireless ids         excessiveAuthAssociation     N
wireless ids         excessiveProbes              N
misc                 savedConfigModified          N
RFController>

RFController>show snmp-server traps wireless-statistics wireless-client
   pktsps-greater-than             disabled
   tput-greater-than               disabled
   avg-bit-speed-less-than         disabled
   avg-signal-less-than            disabled
   nu-percent-greater-than         disabled
   gave-up-percent-greater-than    disabled
   avg-retry-greater-than          disabled
   undecrypt-percent-greater-than  disabled
RFController>

RFController>show snmp-server traps wireless-statistics radio
   pktsps-greater-than             disabled
   tput-greater-than               disabled
   avg-bit-speed-less-than         disabled
   avg-signal-less-than            disabled
   nu-percent-greater-than         disabled
   gave-up-percent-greater-than       disabled
   avg-retry-greater-than             disabled
   undecrypt-percent-greater-than     disabled
   num-stations-greater-than          disabled
RFController>

RFController>show snmp-server traps wireless-statistics wireless-controller
   pktsps-greater-than               disabled
   tput-greater-than                 disabled
   num-stations-greater-than         disabled
RFController>

RFController>show snmp-server traps wireless-statistics wlan
   pktsps-greater-than               disabled
   tput-greater-than                 disabled
   avg-bit-speed-less-than           disabled
   avg-signal-less-than              disabled
   nu-percent-greater-than           disabled
   gave-up-percent-greater-than      disabled
   avg-retry-greater-than            disabled
   undecrypt-percent-greater-than    disabled
   num-stations-greater-than         disabled
RFController>
```

spanning-tree

Common to all modes

Displays Spanning Tree information

Supported in the following platforms:

- Mobility RFS4000 Controller
- Mobility RFS6000 Controller
- Mobility RFS7000 Controller

Syntax

```
show spanning-tree mst [config|detail|instance]
show spanning-tree mst detail interface
[<interface-name>|ge|me1|sa|vlan <1-4094>]
show spanning-tree mst instance <1-15> interface
<IF NAME>||vlan <1-4094>}]
```

Parameters

config	Displays MST configuration information
detail interface [<interface-name>| ge <1-4>|me1|sa<1-4>| vlan <1-4094>]	Displays detailed interface information • <interface-name>– Displays the interface name • ge <1-4> – GigabitEthernet interface • me1 – FastEthernet interface • sa <1-4> – Static Aggregate interface • vlan (1-4094> – Defines the VLAN interface
instance <1-15> [<interface-name>| ge<1-4>|me1|sa<1-4>| vlan <1-4094>]	Displays instance information • <interface-name> – Displays the interface name • vlan <1-4094> – Defines the VLAN interface • ge <1-4> – GigabitEthernet interface • me1 – FastEthernet interface • sa <1-4> – StaticAggregate interface

Example

```
RFController(config)#show spanning-tree mst config
%
% MSTP Configuration Information for bridge 1 :
%--------------------------------------------------------
% Format Id   : 0
% Name      : My Name
% Revision Level : 0
% Digest     : 0xAC36177F50283CD4B83821D8AB26DE62
%--------------------------------------------------------
RFController(config)#

RFController(config)#show spanning-tree mst detail interface ge 2
% Bridge up - Spanning Tree Enabled
% CIST Root Path Cost 0 - CIST Root Port 0 - CIST Bridge Priority 32768
% Forward Delay 15 - Hello Time 2 - Max Age 20 - Max-hops 20
% 1: CIST Root Id 800000157037fabf
% 1: CIST Reg Root Id 800000157037fabf
% 1: CST Bridge Id 800000157037fabf
% portfast bpdu-filter disabled
```

```
% portfast bpdu-guard disabled
% portfast errdisable timeout disabled
% portfast errdisable timeout interval 300 sec
% cisco interoperability configured - Current cisco interoperability off
%  ge2: Port 2002 - Id 87d2 - Role Disabled - State Discarding
%   ge2: Designated External Path Cost 0 -Internal Path Cost 0
%   ge2: Configured Path Cost 20000000  - Add type Explicit ref count 1
%   ge2: Designated Port Id 0 - CST Priority 128  -
%   ge2: CIST Root 0000000000000000
%   ge2: Regional Root 0000000000000000
%   ge2: Designated Bridge 0000000000000000
%   ge2: Message Age 0 - Max Age 0
%   ge2: CIST Hello Time 0 - Forward Delay 0
%   ge2: CIST Forward Timer 0 - Msg Age Timer 0 - Hello Timer 0
%   ge2: Version Multiple Spanning Tree Protocol - Received None - Send STP
%   ge2: No portfast configured - Current  portfast off
%   ge2: portfast bpdu-guard  default  - Current portfast bpdu-guard off
%   ge2: portfast bpdu-filter default  - Current portfast bpdu-filter off
%   ge2: no root guard configured     - Current root guard off
%   ge2: Configured Link Type point-to-point - Current  shared
%
RFController(config)#
```

static-channel-group

Common to all modes

Displays the members of the static channel groups

Supported in the following platforms:

- Mobility RFS7000 Controller
- Mobility RFS4000 Controller

NOTE
This command is not supported on the Mobility RFS6000 Controller

Syntax

```
show static-channel-group
```

Parameters

None

Example

```
RFController(config)#show static-channel-group
RFController(config)#
```

terminal

Common to all modes

Displays the terminal information for the device

Supported in the following platforms:

- Mobility RFS4000 Controller
- Mobility RFS6000 Controller
- Mobility RFS7000 Controller

Syntax

```
show terminal
```

Parameters

None

Example

```
RFController>show terminal
Terminal Type: vt102
Length: 44   Width: 125
RFController>
```

timezone

Common to all modes

Displays the timezone set on the device

Supported in the following platforms:

- Mobility RFS4000 Controller
- Mobility RFS6000 Controller
- Mobility RFS7000 Controller

Syntax

```
show timezone
```

Parameters

None

Example

```
RFController>show timezone
Timezone is Etc/UTC
RFController>
```

traffic-shape

Common to all modes

Displays traffic shaping parameters

Supported in the following platforms:

- Mobility RFS7000 Controller
- Mobility RFS4000 Controller

NOTE
This command is not supported on the Mobility RFS6000 Controller

Syntax

```
show traffic-shape [config|priority-map|statistics]
```

Parameters

[config| priority-map| statistics]	• config class – Displays traffic shaping configuration • statistics class – Displays traffic shaping statistics • class <1-4> – Displays traffic shaping class number • priority-map – Displays .1p to transmit priority map

Example

```
RFController(config)#show traffic-shape priority-map
 802.1p | Shaping priority
   0 | 2
   1 | 0
   2 | 1
   3 | 3
   4 | 4
   5 | 5
   6 | 6
   7 | 7
RFController(config)#
```

users

Common to all modes

Displays a list of users connected to the device

Supported in the following platforms:

- Mobility RFS4000 Controller
- Mobility RFS6000 Controller
- Mobility RFS7000 Controller

Syntax

```
show users
```

Parameters

None

Example

```
RFController>show users
  Line   PID  User    Uptime    Location
  0 con 0 316  admin    06:08:11   ttyS0
 130 vty 0 2308  admin    00:35:18   0
RFController>
```

version

Common to all modes

Displays the current software & hardware version on the device

Supported in the following platforms:

- Mobility RFS4000 Controller
- Mobility RFS6000 Controller
- Mobility RFS7000 Controller

Syntax

```
show version {verbose}
```

Parameters

verbose	Displays software and hardware version information

Example

```
RFController>show version
RFController version 4.3.0.0-046B MIB=01a
Copyright (c) 2009 Brocade, Inc.
Booted from secondary.

Controller uptime is 1 days, 20 hours 53 minutes
RMI XLR V0.4
255476 kB of on-board RAM
```

wireless

Common to all modes

NOTE
The `radio-group` range differs from controller to controller:
Mobility RFS7000 Controller – Supports a range between 0-255
Mobility RFS6000 Controller – Supports a range between 0-64
Mobility RFS4000 Controller – Supports a range between 1-6

Displays the wireless configuration parameters and information

Syntax

```
show wireless [aap-version|ap|ap-containment|
ap-detection-config|ap-images|ap-radio-config|
ap-unadopted||authorized-aps|
channel-power|client|config|country-code-list|default-ap|fw|
hotspot|hotspot-config|ids|ignored-aps|known|mac-auth-local|mesh|mobile-unit|
multicast-packet-limit|
non-preferred-ap-attempts-threshold|phrase-to-key|
qos-mapping|radio|radio-group|regulatory|self-heal-config
|sensor|smart-rf|unauthorized-aps|wips|
wireless-controller-statistics|wlan]
show wireless aap-version
show wireless ap[<LIST>|config [<1-1024>|<MAC>]
show wireless ap-containment [config|table]
show wireless ap-detection-config
show wireless ap-images
show wireless ap-unadopted
show wireless ap-radio-config <MAC>
show wireless approved-aps
show wireless authorized-aps
show wireless channel-power [11a|11b|11bg] [indoor|outdoor]
show wireless client [exclude-list|include-list]
show wireless config
show wireless country-code-list
show wireless default-ap
show wireless hotspot query
show wireless hotspot-config <1-32>
show wireless ids [filter-list|configured-bad-essids
|configure-ap-def-essids|fake-ap-flood threshold|
suspicious ap signal-strength-threshold]
show wireless ignored-aps
show wireless known {ap statistics {<1-1024>}}
show wireless mac-auth-local {<1-1000>}
show wireless mesh statistics {<1-32> {detail}}
show wireless mobile-unit
{[<1-8192>|<MAC>|association-history|association-stats|probe-history|radio|
roaming|statistics|voice|wlan]}
show wireless mobile-unit [<1-8192>|<MAC>|association-stats]
show wireless mobile-unit association-history {<MAC>}
show wireless mobile-unit probe-history [<1-200>|config-list]
show wireless mobile-unit radio <1-4096>
show wireless mobile-unit roaming database
show wireless mobile-unit statistics [<1-4096>|<MAC> {detail}|summary|voice
[<1-4096>|<mac>]]
show wireless mobile-unit voice
show wireless mobile-unit vlan <1-256>
```

```
show wireless multicast-packet-limit
show wireless phrase-to-key [wep64|wep128] <pass-phrase>
show wireless qos-mapping {[wired-to-wireless|
wireless-to-wired]}
show wireless radio
{[<1-4096>|admission-control|all|beacon-table|config|monitor-table|statistics
|unadopted|
uptime|voice]}
show wireless radio
{[<1-4096>|all|beacon-table|monitor-table|unadopted|uptime]}
show wireless radio admission-control voice {<1-4096>}
show wireless radio config {[<1-4096>|default-11a|default-11an|
default-11b|default-11bg|default-11bgn]}
show wireless radio statistics {[<1-4096> {detail}|
long-interval|short-interval|voice {[<1-4096>|long-interval|
short-interval]}}
show wireless radio voice {<1-4096>}
show wireless radio-group {<1-256>}
show wireless regulatory <country code>
show wireless self-heal-config {[<1-4096>|all]}
show wireless sensor {[<1-48>|default-config]}
show wireless smart-rf [calibration-status|configuration|
history|radio]
show wireless smart-rf radio [config|local-status|map|
master-status|neighbors|spectrum] {<1-4096>|<MAC>|
all-11a|all-llbg]}
show wireless unapproved-aps
show wireless unauthorized-aps
show wireless wireless-controller-statistics {detail}
show wireless wlan [config {[<1-256>|all|enabled]}|statistics {<1-256>
{detail}}]
show wireless wips [configured-ap-def-essids|
configured-bad-essids|fake-ap-flood|filter-list|  suspicious-ap]
```

Parameters

aap-version	Displays the minimum adaptive firmware version string

ap [<1-48>|<MAC>|
config [<1-48>|<MAC>]]
	Status of the adopted access point
	• <1-48> – Defines the index of the access point
	• <MAC> – Sets the MAC address of a access point
	• config [<1-1024>|<MAC>] – Status of the configured access point
	  • <1-1024> – AP index from the “show wireless ap” command
	  • <MAC> – MAC address of the ap

ap-containment [config|table]	Rogue AP containment • config – Rogue AP Containment Parameters • table – Rogue AP Containment table
ap-detection-config	Detected AP configuration parameters
ap-images	Displays the access point images on the controller
ap-unadopted	Lists unadopted access points
approved-aps	Displays approved APs detected by access point scans

channel-power [11a|11b|11bg] [indoor|outdoor]	Lists the channels and power levels available for a radio • 11a – Defines the radio as 802.11a • 11b – Defines the radio as 802.11b • 11bg – Defines the radio as 802.11bg These options are available for all the above radio types: • indoor – Radio is placed indoors • outdoor – Radio is placed outdoors
client [exclude-list|include-list]	Wireless client configuration • exclude-list – Sets the exclude list configuration • include-list – Sets the include list configuration
config	Displays wireless configuration information
country-code-list	Displays the list of supported country names and their 2 letter IS0 3166 codes
default-ap	Displays default access-point information
hotspot query	Displays hotspot query string configuration
hotspot-config <1-256>	WLAN hotspot configuration for specified index
ids [configured-bad-essids| filter-list]	Displays intrusion detection configuration parameters • configured-bad-essids – Displays a list of configured bad essids • filter-list – Displays the list of currently filtered wireless clients
known *{ap statistics* {<1-1024>}}	Displays known AP parameters. • ap – Optional. Defines a known AP index <1-1024> • statistics – Optional. Displays known adaptive AP stats • <1-1024> – Optional. Displays adaptive ap statistics for known adaptive APs between 1-1024
mac-auth-local *{<1-1000>}*	Displays mac-auth-local entries for index <1-1000>.
mesh statistics *{<1-32>* {detail}}	Displays mesh related parameters • statistics – Displays mesh statistics • <1-32> – Optional. Defines the mesh index • detail – Optional Displays detailed mesh statistics

wireless-client *{[<1-8192>|<MAC>|association-history|
 	
association-stats|probe-history|radio|roaming|statistics|
voice|wlan]}*
	Displays the parameters of associated wireless clients. All parameters are optional.
	• <1-8192> – Index of wireless client
	• <MAC> – MAC address of wireless client
	• association-history *{<MAC>}*– Displays the association history of the wireless clients with the MAC address and its configured name.
	• association-stats – Displays Statistics of associations and reassociations
	• probe-history [<1-200>|config-list] – Displays the probe history of the wireless client with the address and its configured name
	  • <1-200> – Defines index to display probe-logging
	  • config-list – Lists probe history MAC addresses
	• radio <1-4096> – Displays the associated wireless clients for the radio with the MAC address and its configured name.
	  • Mobility RFS7000 Controller supports <1-4096> radios
	  • Mobility RFS6000 Controller supports <1-1000> radios
	• roaming database – Displays the local wireless-client roaming database.
	• statistics [<1-8192>|<MAC>|summary|voice] – Displays wireless client RF statistics
	  • <1-8192> – Displays Index of wireless-client
	  • <MAC> *{detail}*– Displays MAC address of wireless-client. Optionally display detailed information.
	  • summary – Displays RF-Stats summary of all currently associated wireless-clients
	  • voice [<1-4096>|<MAC>] – Displays wireless-client voice statistics for a radio index or radio MAC address.
	• voice – Displays voice call details
	• wlan <1-256> – Displays the Clients associated to the selected wlan

multicast-packet-limit	Displays the multicast-packet-limit
phrase-to-key [wep128|wep64] <pass-phrase>	Displays the WEP keys generated by a passphrase • wep128 – Displays WEP128 keys • wep64 – Displays WEP64 keys • <pass-phrase> – The passphrase to generate the keys for
qos-mapping *{[wired-to-wireless|wireless-to-wired]}*	Quality of service mappings used for mapping WMM access categories and 802.1p/DSCP tags • wired-to-wireless – Mappings used when traffic is switched from the wired to the wireless side • wireless-to-wired – Mappings used when traffic is switched from the wireless to the wired side

radio *{[<1-4096>|admission-control|all|beacon-table|config|monitor-table|statistics|unadopted|uptime|voice]}*	Radio related commands. All parameters are optional.
	• *<1-4096>* – Defines information on a single radio's index
	• admission-control voice {*<1-4096>*} – Displays summary information for all radios that have admission control enabled. Optionally select the radio.
	• all – Displays information about all radios
	• beacon-table – Displays the radio-to-radio beacon table
	• config {[*<1-4096>*|default-11a|default-11an|default-11b|default-11bg|default-11bgn]} – Displays the selected radio's configuration. All parameters are optional.
	  • <1-4096> – The radio index
	  • default-11a – Default 11a configuration template
	  • default-11an – Default 11an configuration template
	  • default-11b – Default 11b configuration template
	  • default-11bg – Default 11bg configuration template
	  • default-11bgn – Default-11bgn configuration template
	• monitor-table – Displays the radio-to-radio monitoring table
	• statistics {[<1-4094>|long-interval|short-interval|voice]} – Displays a summary of radio statistics. All parameters are optional.
	  • <1-4094> {detail} – Defines a single radio's index. Optionally display the details
	  • long-interval – last 60 minutes for all adopted radios
	  • short-interval – last 30 seconds for all adopted radios
	  • voice {[<1-4096>|long-interval|short-interval]}– Displays voice related statistics for the selected option

	• unadopted – Displays a list of unadopted radios • uptime – Displays the uptime of all adopted radios • voice <1-4094> – Displays voice call details • <1-4094> – Optional. Defines a single radio's index
radio-group *{<1-256>}*	Displays radios in specified group • <1-256> – Optional. A single radio index between < 1-256>. The index range varies based on the controller being used.
regulatory <country-code>	Regulatory (allowed channel/power) information for a particular country. • *<country-code>* – Two character country code for each country
self-heal-config { [<1-4096>|all]}	Sets self healing configuration parameters • *<1-4096>* – Optional. Defines a single radio's index • all – Optional. Defines the self-healing configuration for all radios
sensor *{[<1-48>|default-config]}*	Defines *Wireless Intrusion Protection System* (WIPS) parameters • <1-48> – Specifies the index of a particular sensor to view detailed information about that sensor • default-config – Default configuration parameters for sensors

smart-rf [calibration-status|configuration|history|radio]	Displays smart-rf related management information
	• calibration-status – Displays smart-rf calibration status
	• configuration – Displays smart-rf configuration information
	• history – Displays smart-rf assignment history since last calibration.
	• radio [config|local-status|map|master-status|neighbors|spectrum] *{[<1-4096>|<MAC>|all-11a|all-11bg]}* – Displays smart-rf radio commands.
	  • config – Displays the configuration information
	  • local-status – Displays the local radio status related to smart rf
	  • map – Maps all 11a radios in the configuration
	  • master-status – Displays the radio status from the master radio list. If no parameter is passed, displays status for all radios in the master list
	  • neighbors – Displays the radio's neighbor information
	  • spectrum – Displays all 11a radios spectrum information <1-4096> – The selected radio
	  • <MAC> – The selected radio MAC address
	  • all-11a – All 11a radios
	  • all-11bg – All 11bg radios

unapproved-aps	Defines unapproved APs seen by an access point or a wireless client scan
wireless-controller-statistics *{detail}*	Displays wireless-controller statistics • detail – Optional Displays detailed wireless-controller statistics

wlan [config|statistics]	Displays wireless LAN parameters. The following information is displayed:
	• config [<1-256>|all|enabled] – Displays the wireless LAN configuration information. All parameters optional
	  • <1-256> – The selected wlan
	  • all – all wlans in the configuration
	  • enabled – all wlans that are enabled. Configuration information for disabled wlans are not displayed
	• statistics <1-256> – Displays the wireless LAN statistics for:
	  • <1-256> {detail} – The selected wlan. Optionally display details

wips [configured-ap-def-essids|configured-bad-essids|fake-ap-flood|filter-list|suspicious-ap]	Displays wips parameters
	• configured-ap-def-essids – Displays the list of configured default essids
	• configured-bad-essids – Displays the list of configured bad essids
	• fake-ap-flood threshold – Displays fake-ap flood parameter
	  • threshold – Fake-AP Flood Threshold
	• filter-list – Display the list of currently filtered mobile-units
	• suspicious-ap – Displays suspicious- ap parameters
	  • signal-strength-threshold– Displays signal strength threshold

(config-wireless) Executable Mode

Displays the (config- wireless) configuration parameters and information

Supported in the following platforms:

- Mobility RFS4000 Controller
- Mobility RFS6000 Controller
- Mobility RFS7000 Controller

Syntax

```
show wireless ap [LIST|config]
show wireless config [<1-1024>|LIST]
show wireless radio [<1-4096>|admission-control|all|
beacon-table|config|monitor-table|statistics|unadopted|
uptime|voice]}
show wireless wlan [config|statistics]
show wireless wlan config [<1-256>|all|enabled]
show wireless wlan statistics <1-256> detail
```

Parameters (config-wireless) Executable Mode

show wireless ap [LIST|config]	Displays wireless LAN parameters. The following information is displayed: LIST– MAC address of a single access-port or a list of indices (e.g.1-4,10) for detailed information config [<1-1024>|config] – Displays status of configured access-point <1-1024> – A single ap index LIST – Defines MAC Address of a single access point
show wireless radio [<1-4096>| admission-control|all| beacon-table| config|monitor-table| statistics|unadopted| uptime|voice]}	Refer show wireless radio configuration parameters given in page 106
show wireless wlan [config {all|enabled}| statistics detail} <1-256>	Configures wireless LAN related parameters config [<1-256>|all|enabled] – Configures wlan <1-256> – Displays wlan index all – Displays all the configured wlans enabled – Displays only the currently enabled wlans statistics detail – Displays wlan statistics detail <1-256> – Displays wlan statistics in detail <1-256> – Displays wlan index

Example

```
RFController>show wireless ap
Number of access-points adopted  : 0
Available licenses        : 0
Clustering enabled        : N
Clustering mode         : primary
RFController>
```

```
RFController(config)#show wireless ap config 2
ap mac address : 00-A0-F8-BF-89-45
ap adoption-policy: allow
ap name : AP-00-A0-F8-BF-89-45
ap location : AP-00-A0-F8-BF-89-45-Location
ap on-board-radios: 0
ap secure WISPe mode : disable
ap secure WISPe mode staging : disable
ap shared WISPe secret : 0 defaultS
ap country-code : ""
RFController(config)#

RFController>show wireless ap-detection-config
Rogue  AP timeout   : 300 seconds
Approved AP timeout   : 300 seconds
client-assisted scan     : enabled
client-assisted scan refresh : 300 seconds
configured approved-aps :
Index | Bss Mac      | Ssid
-------------------------------------------------------
Adaptive minimum adoption version: 2.0.0.0-000R
RFController>
RFController>show wireless ap-images
Idx ap-type Image-Name Size (bytes) Version
1 ap300 AP300-WISP 325212 00.02-37
2 ap300 AP300-WISPe 319776 01.00-2281r
3 ap300 AP300-IDS-Sensor 350092 00.00-04
RFController>show wireless ap-unadopted
RFController>

RFController>show wireless approved-aps
access-point detection is disabled
RFController>

RFController>show wireless channel-power 11a indoor
Channel Max Power (dBm) Radar Detected
36      (5180 MHz)  17        -
40      (5200 MHz)  17        -
44      (5220 MHz)  17        -
48      (5240 MHz)  17        -
149     (5745 MHz)  20        -
153     (5765 MHz)  20        -
157     (5785 MHz)  20        -
161     (5805 MHz)  20        -
165     (5825 MHz)  20        -
RFController>

RFController(config)#show wireless ap
Number of access-points adopted : 3
Number of AAPs adopted : 0
Available AP licenses : 45
Available AAP licenses : 0
Redundancy enabled : N
Redundancy mode : active
# MAC               RADIOS[indices] MODEL-NUMBER ADOPTION-MODE STATIC IP
1 00-A0-F8-BF-8A-70 2 [ 3 4 ]       WSAP-5100-100-WW L2        (vlan:10)
2 00-A0-F8-BF-89-45 2 [ 5 6 ]       WSAP-5100-100-WW L2        (vlan:10)
RFController(config)#
```

```
RFController(config)#show wireless config
country-code      : None
secure-wispe-default-secret default
adoption-pref-id    : 1
proxy-arp        : enabled
adopt-unconf-radio   : enabled
dot11-shared-key-auth  : disabled
ap-detection      : disabled
manual-wlan-mapping   : disabled
dhcp sniff state    : disabled
dhcp one portal forward : enabled
dhcp fix broadcast-rsp : disabled
broadcast-tx-speed   : optimize-for-range
wlan bw allocation   : disabled
smart-channels used   :
smart-channels excluded :
Adaptive ap parameters:
 config-apply def-delay : 30 seconds
 config-apply mesh-delay: 3 minutes
wired-to-wireless rate limit per user : unlimited
wireless-to-wired rate limit per user : unlimited
user load balance mode : by-count
secure-wispe-default-secret : default
admission control for voice : enabled
cluster-master-support   : enabled
RFController(config)#

RFController(config)#show wireless config
country-code : us
adoption-pref-id : 1
proxy-arp : enabled
adopt-unconf-radio : enabled
dot11-shared-key-auth : disabled
ap-detection : enabled
manual-wlan-mapping : enabled
dhcp sniff state : disabled
dhcp one portal forward : disabled
dhcp fix broadcast-rsp : disabled
broadcast-tx-speed : optimize-for-range
wlan bw allocation : disabled
smart-channels used : 1,6,11,36,40,44,48,52,56,60,64,100,104,
                      108,112,116,136,140,149,153,157,161,165
smart-channels excluded : 2,3,4,5,7,8,9,10
Adaptive ap parameters:
config-apply def-delay : 30 seconds
config-apply mesh-delay: 180 seconds
user load balance mode : disabled
secure-wispe-default-secret : 0 defaultS
admission control for voice : disabled
cluster-master-support : enabled
nas-id : ""
nas-port-id : ""
wired-to-wireless rate limit per user : unlimited
wireless-to-wired rate limit per user : unlimited
RFController(config)#

RFController>show wireless ids

Detect-window              : 60 seconds
```

```
Violation\Event           Threshold        Filter   Trigger
                                           Ageout
                       MU     RA     SW    (Sec)  A   U   I
Excessive Operations :
probe-requests         30    200      0       0   N   N   -
association-requests   25     45      0       0   N   Y   -
disassociations        25     45      0       0   Y   N   -
authentication-fails   5     20      0        0   N   N   -
crypto-replay-fails    10     25      0       0   N   N   -
80211-replay-fails     10     25      0       0   N   N   -
decryption-fails       25     75      0       0   N   N   -
unassoc-frames         2      0       0       0   N   Y   -
eap-starts            10     20      0        0   N   N   -
eap-naks              10     20      0        0   N   N   -
eap-flood             15     40      0        0   Y   N   -

Anomaly Detection:
null-destination              disabled     0   N   N   N
same-source-destination       disabled     0   N   N   N
multicast-source              disabled     0   N   N   N
weak-wep-iv                   disabled     0   N   N   N
tkip-countermeasures          enabled      0   Y   N   N
invalid-frame-length          enabled      0   Y   N   N
invalid-8021x-frame          disabled      0   N   N   N
invalid-frame-type           enabled       0   Y   N   N
beacon-broadcast-essid       disabled      0   N   N   N
bad-essid-frame              enabled       0   Y   Y   Y
unencrypted-traffic          enabled       0   Y   N   N
non-changing-wep-iv          enabled       0   Y   N   N
detect-adhoc-networks        disabled      0   -   N   N
deauth-broadcast-smac        enabled       0   Y   N   N
invalid-sequence-number      enabled       0   Y   N   N
ap-default-ssid              enabled       0   Y   N   N
identity-theft               enabled       0   Y   -   -
suspicious-ap                enabled       0   -   Y   Y
authorized-dev-in-adhoc-mode enabled       0   Y   -   -
fake-ap-flood                 enabled      0   -   Y   Y
detect-adhoc-with-controller-ssid enabled     0   Y   Y   Y
unauthorized-ap-using-controller-ssid enabled 0   -   Y   Y
RFController#

RFController>show wireless mac-auth-local 50
RFController>

RFController>show wireless wireless-client statistics

wireless-client 1: <00-20-A6-52-5F-83>
WLAN : wlan-1
------ Traffic ----------------------------------------------
           Total Rx Tx

        30s 1hr 30s 1hr 30s 1hr
Pkts per sec:  1.73 0.00 0.87 0.00 0.87 0.00 pps
Throughput:   0.00 0.00 0.00 0.00 0.00 0.00 Mbps
Avg bit speed: 9.19 0.00 Mbps
% Non-unicast pkts: N/A N/A

------ RF Status----------------------------------------------
```

```
           30s 1hr
Avg wireless-client signal: -78.00 0.00 dBm
Avg wireless-client noise: -94.00 0.00 dBm
-- MORE --, next page: Space, next line: Enter, quit: Control-C
Avg wireless-client SNR(dB): 16.00 0.00

------ Errors-----------------------------------------------

           30s 1hr
Avg number of retries: 0.42 0.00
% gave up pkts: 0.00 0.00
% Non-decryptable pkts: 0.00 0.00


RFController(config)#show wireless wireless-client
index  MAC-address    radio type wlan vlan/tunnel ready IP-address  last active
Posture Status
 2   00-0E-9B-98-F9-34 1   11g 1   vlan 1  Y   192.168.2.45  0 Sec
Number of wireless-clients associated: 1
RFController(config)#



RFController(config)#show wireless wireless-client association-history
CLIENT MAC       Radio WLAN Timestamp     Event
============================================================
00-0E-9B-98-F9-34 1   1   1116316     Association
00-0E-9B-98-F9-34 1   1   12248923    Unassociation
00-0E-9B-98-F9-34 1   1   12250053    Association
00-0E-9B-98-F9-34 1   1   4280690527  Unassociation
00-0E-9B-98-F9-34 1   1   4280691647  Association
00-0E-9B-98-F9-34 1   1   4280716777  Unassociation
00-0E-9B-98-F9-34 1   1   4280717937  Association
RFController(config)#

RFController(config)#show wireless wireless-client radio 1
index  MAC-address    radio type wlan vlan/tunnel ready IP-address  last active
Posture Status
 2   00-0E-9B-98-F9-34 1   11g 1   vlan 1  Y   192.168.2.45  0 Sec
Listed 1 of a total of 1 wireless-clients
RFController(config)#

RFController(config)#show wireless wlan config 1
#enabled  ssid authentication encryption vlan(s) description
5    Y    TechDoc_02       none         wep128      2      TechDoc_Test_02
6    Y      TechDoc_01       none      wep128    1      TechDoc_Test_01
8    N      TechDoc_02       none      none    1      WLAN8
----
RFController(config)#
RFController(config)#show wireless wlan config 5

RFController(config)#show wireless wlan config 8

WLAN: 8, status: disabled, description: WLAN8, ssid: TechDoc_02
 auth: none, encr: none
 inactivity-timeout      : 1800 seconds
 hold-time               : 5 seconds
 nas-id                  : ""
 nas-port-id             : ""
 vlan    1               : unlimited users
```

```
 query                    :
 smart-channels used      : 1,6,11,36,40,44,48,149,153,157,161,165
 smart-channels excluded : 2,3,4,5,7,8,9,10
 mu-mu-disallow: disabled, secure-beacon: disabled, answer-bcast-ess: enabled,
 weight: 1, prioritize-voice: disabled, spectralink-voice-protocol: disabled
 multicast mask1: 00-00-00-00-00-00, mask2: 00-00-00-00-00-00
 traffic-classification : normal, wmm-mapping: 8021p, L3-mobility: disabled
 rate-limit: wired-to-wireless: unlimited wireless-to-wired: unlimited
 Client Bridge Backhaul is disabled on this WLAN
 This WLAN is an extended WLAN
 NAC Mode: none
RFController(config)#

RFController(config-wireless)#show wireless ap
Number of access-ports adopted   : 0
Number of AAPs adopted           : 0
Available AP licenses            : 0
Available AAP licenses           : 0
Redundancy enabled               : N
Redundancy mode                  : active
RFController(config-wireless)#

RFController(config-wireless)#show wireless wlan config 9

WLAN: 9, status: disabled, description: WLAN9, ssid: 109
 auth: none, encr: none, mfp: none
 inactivity-timeout      : 1800 seconds
 hold-time               : 5 seconds
 nas-id                  : ""
 nas-port-id             : ""
 vlan    1               : unlimited users
 query                   :
 smart-channels used     : 1,6,11,36,40,44,48,52,56,60,64,149,153,157,161
 smart-channels excluded : 2,3,4,5,7,8,9,10,12,13
 mu-mu-disallow: disabled, secure-beacon: disabled, answer-bcast-ess: enabled,
 weight: 1, prioritize-voice: disabled, spectralink-voice-protocol: disabled
 multicast mask1: 00-00-00-00-00-00, mask2: 00-00-00-00-00-00
 traffic-classification : normal, wmm-mapping: 8021p, L3-mobility: disabled
 rate-limit: wired-to-wireless: unlimited wireless-to-wired: unlimited
 Client Bridge Backhaul is disabled on this WLAN
 This WLAN is an extended WLAN
 url-logging: disabled
 Enforce-Dhcp: disabled
 NAC Mode: none

RFController(config)#show wireless wireless-controller-statistics detail
Rates(Mbps) Tx packets Rx Packets
---------------------------------------- ---------- -------
802.11b rates (1, 2, 5.5, 6) 0 0
802.11a/g low rates (9, 11, 12) 0 0
802.11a/g low rates (18, 22, 24) 0 0
Common Commands 2-119
802.11a/g high rates (36, 48, 54) 0 0
802.11n (MCS 0-3) 0 0
802.11n (MCS 4-7) 0 0
802.11n (MCS 8-11) 0 0
802.11n (MCS 12-15) 0 0
Voice:
Rates(Mbps) Tx packets Rx Packets
---------- ---------- ----------
```

```
1.0               0          0
2.0               0           0
5.5               0           0
6.0               0           0
9.0               0           0
11.0              0           0
12.0              0           0
18.0              0           0
22.0              0           0
24.0              0           0
36.0              0           0
48.0              0           0
54.0              0           0
Retry Counts Packets
------------ -------
    0          0
    1          0
    2          0
    3          0
    4          0
    5          0
    6          0
    7          0
    8          0
    9          0
    10         0
    11         0
    12         0
RFController(config)#
RFController(config)#show wireless radio statistics 3
***** Radio-3 *********************
mobile-units Associated : 0 Voice Prioritized : 0
------ Traffic -------------------------------------------------
Total                     Rx           Tx
---------------- ---------------- --------
30s 1hr               30s 1hr       30s 1hr
Pkts per sec: 0.00 0.00 0.00 0.00
0.00 0.00 pps
Throughput: 0.00 0.00 0.00 0.00
0.00 0.00 Mbps
Avg bit speed: 0.00 0.00 Mbps
% Non-unicast pkts: 0.00 0.00
------ RF Status-----------------------------------------------
30s 1hr
Avg mobile-unit signal: 0.00 0.00 dBm
Avg mobile-unit noise: -92.25 -93.50 dBm
Avg mobile-unit SNR(dB): 92.25 93.50
------ Errors---------------------------------------------------
30s 1hr
Avg number of retries: 0.00 0.00
% gave up pkts: 0.00 0.00
% Non-decryptable pkts: 0.00 0.00
------ Voice----------------------------------------------------
30s 1hr
Voice MUs - Avg: 0.00 0.00
Voice MUs - Max: 0.00 0.00
% gave up voice pkts: 0.00 0.00
RFController(config)#show wireless radio statistics 3 detail
Voice
Rates(Mbps) Tx packets Rx Packets Tx packets Rx Packets
```

```
----------- ---------- ---------- ---------- ----------
1.0              2          0          0          0
2.0              0          0          0          0
5.5              0          0          0          0
6.0              0          0          0          0
9.0              0          0          0          0
11.0             0          0          0          0
12.0             0          0          0          0
18.0             0          0          0          0
22.0             0          0          0          0
24.0             0          0          0          0
36.0             0          0          0          0
48.0             0          0          0          0
54.0             0          0          0          0
Retry Counts Packets
------------ -------
    0           2
    1           0
    2           0
    3           0
    4           0
    5           0
    6           0
    7           0
    8           0
    9           0
    10          0
    11          0
    12          0
    13          0
    14          0
    15          0
Voice failed : 0
Tx BCMC drops : 0
RFController(config)#
RFController(config)#show wireless wlan statistics 2
mobile-units Associated : 0 Radios active : 6
Voice mobile-units Associated : 0
------ Traffic ----------------------------------------------------
Total                    Rx           Tx
---------------- ---------------- --------
30s 1hr               30s 1hr       30s 1hr
Pkts per sec: 0.00 0.00 0.00 0.00
0.00 0.00 pps
Throughput: 0.00 0.00 0.00 0.00
0.00 0.00 Mbps
Avg bit speed: 0.00 0.00 Mbps
% Non-unicast pkts: 0.00 0.00
------ RF Status----------------------------------------------------
30s 1hr
Avg mobile-unit signal: 0.00 0.00 dBm
Avg mobile-unit noise: 0.00 0.00 dBm
Avg mobile-unit SNR(dB): 0.00 0.00
------ Errors-------------------------------------------------------
30s 1hr
Avg number of retries: 0.00 0.00
% gave up pkts: 0.00 0.00
% Non-decryptable pkts: 0.00 0.00
RFController(config)#
RFController(config)#show wireless mobile-unit statistics 00-A0-F8-
```

```
BF-61-6E
***** mobile-unit 1: <00-A0-F8-BF-61-6E>********************
WLAN : wlan-4
------ Traffic ----------------------------------------------------
Total Rx
Tx
---------------- ---------------- --------
30s 1hr 30s 1hr 30s
1hr
Pkts per sec: 0.00 0.01 0.00 0.00
0.00 0.00 pps
Throughput: 0.00 0.00 0.00 0.00
0.00 0.00 Mbps
Avg bit speed: 0.00 1.51 Mbps
% Non-unicast pkts: 0.00 71.43
------ RF Status----------------------------------------------------
30s 1hr
Avg mobile-unit signal: -82.00 -81.00 dBm
Avg mobile-unit noise: -92.00 -94.50 dBm
Avg mobile-unit SNR(dB): 10.00 13.50
------ Errors----------------------------------------------------
30s 1hr
Avg number of retries: 0.00 2.00
% gave up pkts: 0.00 0.00
Common Commands 2-123
% Non-decryptable pkts: 0.00 0.00
RFController(config)#show wireless mobile-unit statistics 00-A0-F8-
BF-61-6E detail ?
| Output modifiers
> Output redirection
>> Output redirection appending
<cr>
RFController(config)#
RFController(config)#show wireless mobile-unit statistics 00-A0-F8-
BF-61-6E detail
mu_idx = 0
Retry Counts Packets
------------ -------
    0          0
    1          0
    2          0
    3          0
    4          1
    5          1
    6          0
    7          1
    8          0
    9          0
    10         0
    11         0
    12         0
    13         0
    14         0
    15         0
Voice failed : 0
```

wlan-acl

Common to all modes

Displays the WLAN based access control list information

Supported in the following platforms:

- Mobility RFS4000 Controller
- Mobility RFS6000 Controller
- Mobility RFS7000 Controller

Syntax

```
show wlan-acl [<1-256>|all]
```

Parameters

wlan-acl [<1-256>|all]	Displays WLAN based access control list information • <1-256> – Displays ACLs attached to the specified WLAN ID • all – Displays all ACLs attached to a WLAN port

Example

```
RFController>show wlan-acl 20
WLAN port: 20
 Inbound IP Access List  :
 Inbound MAC Access List :
 Outbound IP Access List :
 Outbound MAC Access List :
RFController>

RFController>show wlan-acl all
WLAN port: 1
 Inbound IP Access List  :78
 Inbound MAC Access List :200
 Outbound IP Access List :78
 Outbound MAC Access List :200
RFController>
```

access-list

Privilege / Global Config

Displays the access lists (numbered and named) configured on the controller. The numbered access list displays numbered ACLs. The named access list displays named ACL details.

Supported in the following platforms:

- Mobility RFS4000 Controller
- Mobility RFS6000 Controller
- Mobility RFS7000 Controller

Syntax

```
show access-list [<1-99>|<100-199>|<1300-1999>|
<2000-2699>|<acl-name>]
```

Parameters

access-list [<1-99>|<100-199>|<1300-1999>|<2000-2699>|<acl-name>]	Displays access-list entries. • <1-99> - IP standard access list • <100-199> - IP extended access list • <1300-1999> - IP standard access list (expanded range) • <2000-2699> – IP extended access list (expanded range) • <acl-name> - Name of ACL

Example

```
RFController(config)#show access-list
Extended IP access list 110
  permit ip 192.168.1.0/24 192.168.100.0/24 rule-precedence 5
  permit ip 192.168.63.0/24 192.168.100.0/24 rule-precedence 63
  permit ip 192.168.157.0/24 192.168.100.0/24 rule-precedence 157
RFController(config)#

RFController(config)#show access-list 110
Extended IP access list 110
  permit ip 192.168.1.0/24 192.168.100.0/24 rule-precedence 5
  permit ip 192.168.63.0/24 192.168.100.0/24 rule-precedence 63
  permit ip 192.168.157.0/24 192.168.100.0/24 rule-precedence 157
RFController(config)#
```

aclstats

Privilege / Global Config

Displays the statistics of configured access lists

Supported in the following platforms:

- Mobility RFS4000 Controller
- Mobility RFS6000 Controller
- Mobility RFS7000 Controller

Syntax

show aclstats [access-list|vlan <1-4094>]

```
show aclstats {<1-99>|<100-199>|<1300-1999>|<2000-2699>|
<acl-name>}
show aclstats vlan <1-4094>
```

Parameters

access-list {<1-99>|<100-199>|<1300-1999>|<2000-2699>|<acl-name>}	Displays configured access lists. • <1-99> - IP standard access list • <100-199> - IP extended access list • <1300-1999> - IP standard access list (expanded range) • <2000-2699> - IP extended access list (expanded range) • <acl-name> - Name of ACL
vlan <1-4094>	• Defines the VLAN interface (between 1- 4094)

Example

```
RFController(config)#show aclstats vlan 400
RFController(config)#
```

alarm-log

Privilege / Global Config

Displays the contents of the alarm log on the device

Supported in the following platforms:

- Mobility RFS4000 Controller
- Mobility RFS6000 Controller
- Mobility RFS7000 Controller

Syntax

```
show alarm-log {<1-65535>|acknowledged|all|count|new|
severity-to-limit}
show alarm-log severity-to-limit {critical|
 informational|major|normal|warning}
```

Parameters

alarm-log [<1-65535>| acknowledged|all|count|new| severity-to-limit]	Displays the contents of the alarm log on the device.
	• <1-65535> – Displays the details of a specific alarm ID
	• acknowledged – Displays information for acknowledged alarms currently in the system
	• all – Displays all the alarms currently in the system
	• count – Displays the number (count) of the alarms currently in the system
	• new – Displays those new alarms currently in the system
	• severity-to-limit {critical|informational major|normal|warning} – Displays the alarms having specified severity, as well as those alarms with a severity higher than the specified value.
	  • critical – Displays all critical alarms
	  • informational – Displays all informational or higher severity alarms
	  • major – Displays all major or higher severity alarms
	  • normal – Displays all normal or higher severity alarms
	  • warning - Displays all warning or higher severity alarms

boot

Privilege / Global Config

Displays the boot configuration of the device

Supported in the following platforms:

- Mobility RFS4000 Controller
- Mobility RFS6000 Controller
- Mobility RFS7000 Controller

Syntax

```
show boot
```

Parameters

None

Example

```
RFController#show boot

Image      Build Date            Install Date          Version
-----      --------------------  --------------------  --------------
Primary    Oct 16 03:55:43 2008  Sep 15 00:53:56 2008  4.2.1.0
Secondary  Sep 30 00:14:30 2008  Aug 27 01:46:32 2008  4.2.1.0

Current Boot      : Primary
Next Boot         : Primary
Software Fallback : EnabledRFController#
```

clock

Privilege / Global Config

Displays the system clock

Supported in the following platforms:

- Mobility RFS4000 Controller
- Mobility RFS6000 Controller
- Mobility RFS7000 Controller

Syntax

```
show clock
```

Parameters

None

Example

```
RFController#show clock
Jun 01 00:51:34 UTC 2010
RFController#
```

debugging

Privilege / Global Config

Displays the debugging configuration information

Supported in the following platforms:

- Mobility RFS4000 Controller
- Mobility RFS6000 Controller
- Mobility RFS7000 Controller

Syntax

```
show debugging mstp
```

Parameters

mstp	Displays the current MSTP configuration

Example

```
RFController(config)#show debugging mstp
MSTP debugging status:
RFController(config)#
```

dhcp

Privilege / Global Config

Displays existing DHCP server configurations

Supported in the following platforms:

- Mobility RFS4000 Controller
- Mobility RFS6000 Controller
- Mobility RFS7000 Controller

Syntax

```
show dhcp [config|status]
```

Parameters

config	Displays the current DHCP server configuration
status	Displays whether the DHCP server is running

Example

```
RFController#show dhcp config

service dhcp
!
ip dhcp pool vlan6
 default-router xxx.xxx.xxx.2
 network xxx.xxx.xx.0/24
 address range xxx.xxx.xx.xx aaa.aaa.aa.aa

RFController#
```

file

Privilege / Global Config

Displays the file system information

Supported in the following platforms:

- Mobility RFS4000 Controller
- Mobility RFS6000 Controller
- Mobility RFS7000 Controller

Syntax

```
show file [information|systems]
```

Parameters

file [information|systems]	Displays the filesystem information. • information <FILE> – Displays file information • systems – Lists existing filesystems

Example

```
RFController#show file systems
File Systems:

   Size(b)   Free(b)   Type Prefix
      -         -  opaque system:
  13704192  11904000  flash nvram:
  19524608  16866304  flash flash:
      -         - network sftp:
      -         - network http:
      -         - network ftp:
      -         - network tftp:
RFController#
```

ftp

Privilege / Global Config

Displays the FTP server configuration

Supported in the following platforms:

- Mobility RFS4000 Controller
- Mobility RFS6000 Controller
- Mobility RFS7000 Controller

Syntax

```
show ftp
```

Parameters

None

Example

```
RFController#show ftp
FTP Server: Disabled
User Name: anonymous or ftpuser
Password:  ********
Root dir:  flash:/
RFController#
```

password-encryption

Privilege / Global Config

Displays the global password encryption status

Supported in the following platforms:

- Mobility RFS4000 Controller
- Mobility RFS6000 Controller
- Mobility RFS7000 Controller

Syntax

```
show password-encryption status
```

Parameters

status	Displays the existing password-encryption status

Example

```
RFController#show password-encryption status
Password encryption is disabled
RFController#
```

running-config

Privilege / Global Config

Displays the contents of those configuration files wherein all configured MAC and IP access lists are applied to an interface

Supported in the following platforms:

- Mobility RFS4000 Controller
- Mobility RFS6000 Controller
- Mobility RFS7000 Controller

Syntax

```
show running-config [full|include-factory]
```

Parameters

running-config [full|include-factory]	Displays the contents of the configuration files • full – Displays the file's full (complete) configuration • include-factory – Includes factory defaults

Example

```
RFController(config)#show running-config full
!
! configuration of Mobility RFS7000 version 4.3.0.0
!
version 1.3
!!
aaa authentication login default local none
service prompt crash-info
!
network-element-id RFS7000
!
username "admin" password 1 8e67bb26b358e2ed20fe552ed6fb832f397a507d
username "admin" privilege  superuser
username "operator" password 1 fe96dd39756ac41b74283a9292652d366d73931f
!
!
!
spanning-tree mst cisco-interoperability enable
spanning-tree mst configuration
 name My Name
!
country-code us
logging buffered 4
logging console 4
snmp-server engineid netsnmp 6b8b456749d9e5c1
snmp-server sysname RFS7000
snmp-server manager v2
snmp-server manager v3
snmp-server user snmptrap v3 encrypted auth md5 0x22b4e8506bf66b435abdde2
b996e8100
snmp-server user snmpmanager v3 encrypted auth md5 0x22b4e8506bf66b435abd
de2b996e8100
snmp-server user snmpoperator v3 encrypted auth md5 0x0153e87f2d43032f221
b1f3e340942d2
```

```
firewall dhcp-snoop-conflict-detection disable
firewall dhcp-snoop-conflict-logging disable
ip http server
ip http secure-trustpoint default-trustpoint
ip http secure-server
ip ssh
ip telnet
no service pm sys-restart
!
wireless
 secure-wispe-default-secret 0 defaultS
 no ap-ip default-ap controller-ip
 smart-rf
 wireless
 !
!
radius-server local
!
interface ge1
 controllerport access vlan 1
 ip dhcp trust
!
interface ge2
 controllerport access vlan 1
 ip dhcp trust
!
interface ge3
 controllerport access vlan 1
 ip dhcp trust
!
interface ge4
 controllerport access vlan 1
 ip dhcp trust
!
interface me1
 ip address 10.1.1.100/24
!
interface vlan1
 ip address 172.16.10.2/24
!
rtls
 rfid
 espi
 sole
!
line con 0
line vty 0 24
!
end

RFController(Config)#

RFController(config)#show running-config include-factory
!
! configuration of RFController version 4.0.0.0-008D
!
version 1.0
!
service prompt crash-info
no service set command-history
```

```
no service set reboot-history
no service set upgrade-history
!
hostname RFController
!
banner motd Welcome to CLI!
username admin password 1 8e67bb26b358e2ed20fe552ed6fb832f397a507d
username admin access console web ssh telnet
username admin privilege superuser
username operator password 1 fe96dd39756ac41b74283a9292652d366d73931f
username operator access console web ssh telnet
username operator privilege monitor
!
!
!
!
spanning-tree mst config
 name My Name
!
no management secure
ip domain-lookup
service diag period 1000
service diag enable
country-code us
redundancy group-id 1
redundancy interface-ip 0.0.0.0
redundancy mode primary
redundancy hold-period 15
redundancy heartbeat-period 5
redundancy discovery-period 30
no redundancy handle-stp enable
no redundancy dhcp-server enable
no redundancy enable
.............................................
.............................................
no radio default-11b enhanced-beacon-table
no radio default-11b enhanced-probe-table
no radio 1 neighbor-smart-scan
no radio 2 neighbor-smart-scan
no ap-detection enable
.............................................
.............................................
ip address 123.111.2.1/24
 no ip helper-address
!
sole
 no adapter AeroScout enable
!
radius-server retransmit 3
radius-server timeout 5
radius-server key
!
aaa authentication login default local none
line con 0
line vty 0 24
!
end

RFController(config)#
```

securitymgr

Privilege / Global Config

Displays the security manager event-logs

Supported in the following platforms:

- Mobility RFS4000 Controller
- Mobility RFS6000 Controller
- Mobility RFS7000 Controller

Syntax

```
show securitymgr event-logs
```

Parameters

None

Example

```
RFController#show securitymgr event-log
RFController#
```

sessions

Privilege / Global Config

Displays the list of current active open sessions on the device

Supported in the following platforms:

- Mobility RFS4000 Controller
- Mobility RFS6000 Controller
- Mobility RFS7000 Controller

Syntax

```
show sessions
```

Parameters

None

Example

```
RFController#show sessions
SESSION  USER    LOCATION    IDLE     START TIME
  1    cli  Console      06:24m   May 31 18:31:36 2010
** 2    cli  10.10.10.1    00:00m   Jun 1 00:04:30 2010
RFController#
```

startup-config

Privilege / Global Config

Displays the complete startup configuration script on the console

Supported in the following platforms:

- Mobility RFS4000 Controller
- Mobility RFS6000 Controller
- Mobility RFS7000 Controller

Syntax

```
show startup-config
```

Parameters

None

Example

```
RFController(config)#show startup-config
!
! configuration of Mobility RFS7000 version 4.3.0.0
!
version 1.3
!
!
aaa authentication login default local none
service prompt crash-info
!
network-element-id RFS7000
!
username "admin" password 1 8e67bb26b358e2ed20fe552ed6fb832f397a507d
username "admin" privilege  superuser
username "operator" password 1 fe96dd39756ac41b74283a9292652d366d73931f
!
!
!
spanning-tree mst cisco-interoperability enable
spanning-tree mst configuration
 name My Name
!
country-code us
logging buffered 4
logging console 4
snmp-server engineid netsnmp 6b8b456749d9e5c1
snmp-server sysname RFS7000
snmp-server manager v2
snmp-server manager v3
snmp-server user snmptrap v3 encrypted auth md5 0x22b4e8506bf66b435abdde2
b996e8100
snmp-server user snmpmanager v3 encrypted auth md5 0x22b4e8506bf66b435abd
de2b996e8100
snmp-server user snmpoperator v3 encrypted auth md5 0x0153e87f2d43032f221
b1f3e340942d2
firewall dhcp-snoop-conflict-detection disable
firewall dhcp-snoop-conflict-logging disable
ip http server
```

```
ip http secure-trustpoint default-trustpoint
ip http secure-server
ip ssh
ip telnet
no service pm sys-restart
!
wireless
 secure-wispe-default-secret 0 defaultS
 no ap-ip default-ap controller-ip
 smart-rf
 wireless
 !
!
radius-server local
!
interface ge1
 controllerport access vlan 1
 ip dhcp trust
!
interface ge2
 controllerport access vlan 1
 ip dhcp trust
!
interface ge3
 controllerport access vlan 1
 ip dhcp trust
!
interface ge4
 controllerport access vlan 1
 ip dhcp trust
!
interface me1
 ip address 10.1.1.100/24
!
interface vlan1
 ip address 172.16.10.2/24
!
rtls
 rfid
 espi
 sole
!
line con 0
line vty 0 24
!
end

RFController#
```

upgrade-status

Privilege / Global Config

Displays the last image-upgrade status

Supported in the following platforms:

- Mobility RFS4000 Controller
- Mobility RFS6000 Controller
- Mobility RFS7000 Controller

Syntax

```
show upgrade-status {detail}
```

Parameters

None

Example

```
RFController#show upgrade-status
Last Image Upgrade Status : Successful
Last Image Upgrade Time  : Mon May 21 16:27:40 2010
RFController#
```

mac-name

User/Privilege Exec

Displays the configured MAC name

Supported in the following platforms:

- Mobility RFS4000 Controller
- Mobility RFS6000 Controller
- Mobility RFS7000 Controller

Syntax

```
show mac-name
```

Parameters

None

Example

```
RFController(config-wireless)#show mac-name
Index  MAC Address    MAC Name
 1   00-18-DE-82-78-6B GE1PortMACAddress
Number of MAC names configured = 1
RFController(config-wireless)#
```

firewall

Priv Exe Mode

Displays wireless firewall

Supported in the following platforms:

- Mobility RFS4000 Controller
- Mobility RFS6000 Controller
- Mobility RFS7000 Controller

Syntax

```
show firewall [config|dhcp|flow]
show firewall [config|dhcp snoop-table|flow timeouts]
```

Parameters

firewall [config| dhcp snoop-table| flow timeouts]	Displays firewall configuration information. • config – Displays Configuration • dhcp snoop-table - Displays DHCP snoop table entries • flow timeouts – Displays firewall flow timeout configuration

Example

```
RFController#show firewall
RFController#

RFController#show firewall config
RFController#

RFController#show firewall flow
RFController#
```

NOTE
For information on the 'firewall' command in Global Config mode, refer to *firewall on page 316*.

role

Priv Exe Mode

Displays existing role name

Supported in the following platforms:

- Mobility RFS4000 Controller
- Mobility RFS6000 Controller
- Mobility RFS7000 Controller

Syntax

```
show role [<role-name>|wireless-clients]
```

Parameters

role [<role-name>| wireless-clients]	Displays existing role name • <role-name> – Displays existing role name • wireless-clients – Displays wireless-clients assigned with these roles

Example

```
RFController#show role
RFController#

RFController#show role word
RFController#

RFController#show role wireless-clients
RFController#
```

virtual-IP

Global Config Mode

Supported in the following platforms:

- Mobility RFS4000 Controller
- Mobility RFS6000 Controller
- Mobility RFS7000 Controller

Syntax

```
show virtual-ip [config|status]
```

Parameters

show virtual-ip [config|status]	Displays all the virtual-ip's present in the configuration. config – Displays the configuration details. status – Displays current status of the controller.

Example

```
RFController>show virtual-ip status
VIP State                    : VIP_ST_INIT
VIP Status                   : Disabled
Cluster Redundancy Status    : Disabled
Advertisement Length         : 0
Total Advertisements Sent    : 0
Total Number of Peers        : 0
Total Learning Advts Sent    : 0
Total Advertisements Recvd   : 0
Reserved VMAC Address Range  : 00-15-70-88-8A-90 to 00-15-70-88-8B-8F
Used VMAC Address Range      : 00-15-70-88-8A-90 to 00-15-70-88-8A-90
Available VMAC Address Count : 256
Used VMAC Address Count      : 0
DHCP Server status           : Not Running on this Controller
============================================================
Vlan | Priority | controllerID | State |  Advt sent  |   Advt recvd
RFController>

RFController>show virtual-ip config
RFS7K-1(config)#show virtual-ip config
Virtual-IP Status           : Enabled
Cluster Redundancy Status   : Enabled
Priority Selection Mode     : Automatic
Learning Timeout(sec)       : 2
Advertisement Timeout(sec)  : 1
Gratuitous ARP Timeout(sec) : 180
Virtual-IP Server Port      : 51525
Controller IP               : 192.168.11.4
Reserved VMAC Address Range : 00-15-70-88-8A-90 to 00-15-70-88-8B-8F
Configured Virtual MAC      : 00-15-70-88-8A-98
DHCP Server status          : Active
+-------------------------------------------------+
| Vlan |  Priority  |  ControllerIP |  Virtual IP   |
-------------------------------------------------+
|   11 | 3232238340 |192.168.11.4   |192.168.11.10  |
+-------------------------------------------------
```

```
RFController>
RFS7K-1(config)#show virtual-ip status
Virtual-IP State             : Master
Virtual-IP Config Status     : Enabled
Virtual-IP Runtime Status    : Enabled
Cluster Redundancy Status    : Enabled
Advertisement Length         : 176
Total Advertisements Sent    : 1619309
Total Learning Advts Sent    : 0
Total Advertisements Recvd   : 0
DHCP Server status           : Active
Total Number of Peers        : 1
Peer Status Information      :
+-------------------------------------------------------------------------+
|    Peer IP      |  Status  |     Advts Sent    |    Advts Recvd       |
+-------------------------------------------------------------------------+
| 192.168.11.5    | Slave    |     600214        |    0                 |
+-------------------------------------------------------------------------+
Virtual IP Master Details    :
+-------------------------------------------------+
| Vlan |  Priority | ControllerID  |  Virtual IP   |
--------------------------------------------------+
|11    | 3232238340|   192.168.11.4|  192.168.11.10|
+-------------------------------------------------+
RFController>
RFS7K-1(config)#no virtual-ip all
  all     Remove all VIP entries
  enable  Disable IP Redundancy protocol
  vlan    VLAN of the Virtual IP
  vmac    Virtual MAC
```

NOTE

On executing the above command, all the virtual-ip entries configured on the Controller will be removed.

```
RFS7K-1(config)#no virtual-ip enable
```

Disables the virtual-ip protocol

```
RFS7K-1(config)#no virtual-ip vlan 1
```

Removes the configured virtual-ip of that vlan

```
RFS7K-1(config)#no virtual-ip vmac
```

Removes the configured vmac on the controller

wwan

Common to all modes

Configures wireless wan feature

Supported in the following platforms:

- Mobility RFS4000 Controller
- Mobility RFS6000 Controller
- Mobility RFS7000 Controller

Syntax

```
show wwan [config|dns-server]
```

Parameters

config	Displays wwan signal configuration
dns-server	Displays wwan DNS server addresses

Example

```
RFController#show wwan config
Access Point Name : isp.cingular
Auth-type: chap
Username : isp@cingulargprs.com
RFController#

RFController#show wwan dns-server
Preferred DNS server : 209.183.54.151
Alternate DNS server : 209.183.54.151
RFController#

 RFController#show interfaces wwan
Interface wan
Hardware Type PPP, Interface Mode Layer 3
index=8, metric=1, mtu=1500, (PAL-IF)
<UP,POINTOPOINT,RUNNING,NOARP,MULTICAST>
inet 166.129.246.245/32 pointopoint 10.64.64.64
input packets 0, bytes 0, dropped 0, multicast packets 0
input errors 0, length 0, overrun 0, CRC 0, frame 0, fifo 0, missed 0
output packets 184, bytes 17618, dropped 0
output errors 0, aborted 0, carrier 0, fifo 0, heartbeat 0, window 0
collisions 0
RFController#

RFController#show ip interface brief
Interface        IP-Address/Mask  Status    Protocol
me1              10.1.1.100/24      up       down
vlan1            192.168.1.1/24     up       up
vlan11           192.168.11.1/24     up      up
vlan2            64.171.249.249/24  up      up
wan              166.129.246.245/32 up      up
RFController#
```

aap-wlan-acl

Privilege / Global Config

Supported in the following platforms:

- Mobility RFS4000 Controller
- Mobility RFS6000 Controller
- Mobility RFS7000 Controller

Syntax

In Mobility RFS4000 Controller,

```
show aap-wlan-acl [<1-24>|all]
```

In Mobility RFS6000 Controller,

```
show aap-wlan-acl [<1-32>|all]
```

In Mobility RFS7000 Controller,

```
show aap-wlan-acl [<1-256>|all]
```

Parameters

aap-wlan-acl [<1-32>|all]	Applies an ACL on wlan for an aap. <1-32> – Displays ACLs attached to the specified wlan id for aap all – Displays ACLs attached to wlan port

Example

```
RFController(config)#show aap-wlan-acl 8
RFController(config)#
```

aap-wlan-acl-stats

Privilege / Global Config

Supported in the following platforms:

- Mobility RFS4000 Controller
- Mobility RFS6000 Controller
- Mobility RFS7000 Controller

Syntax

```
show aap-wlan-acl-stats
```

Parameters

aap-wlan-acl-stats	Displays IP filtering wlan based statistics

Example

```
RFController(config)#show aap-wlan-acl-stats
RFController(config)#
```

protocol-list

Common to all Modes

Supported in the following platforms:

- Mobility RFS4000 Controller
- Mobility RFS6000 Controller
- Mobility RFS7000 Controller

Syntax

```
show protocol-list
```

Parameters

show protocol-list	Displays the list of protocols

Example

```
RFController(config)#show protocol-list
Protocol Name          Protocol Number
ip                     0
icmp                   1
igmp                   2
ggp                    3
ipencap                4
st                     5
tcp                    6
egp                    8
igp                    9
pup                    12
udp                    17
hmp                    20
xns-idp                22
rdp                    27
iso-tp4                29
xtp                    36
ddp                    37
idpr-cmtp              38
ipv6                   41
ipv6-route             43
ipv6-frag              44
RFController(config)#
```

service-list

Common to all Modes

Supported in the following platforms:

- Mobility RFS4000 Controller
- Mobility RFS6000 Controller
- Mobility RFS7000 Controller

Syntax

```
show service-list
```

Parameters

show service-list	Displays the list of services

Example

```
RFController#show service-list
Service Name            Port Number
tcpmux                  1/tcp
rtmp                    1/ddp
nbp                     2/ddp
echo                    4/ddp
zip                     6/ddp
echo                    7/tcp
echo                    7/udp
discard                 9/tcp
discard                  9/udp
systat                   11/tcp
daytime                  13/tcp
daytime                  13/udp
telnet                   23/tcp
smtp                     25/tcp
RFController#
```

Chapter

User Exec Commands

3

In this chapter

Logging in to the controller places you within the USER EXEC command mode. Typically, a login requires a user name and password. You have three login attempts before a connection attempt is refused. USER EXEC commands (available at the user level) are a subset of the commands available at the privileged level. In general, USER EXEC commands allow you to connect to remote devices, perform basic tests and list system information.

To list available USER EXEC commands, use **?** at the command prompt. The USER EXEC prompt consists of the device host name followed by an angle bracket (**>**). The default host name is generally “WLAN Module”. Use the GLOBAL CONFIG command to change the hostname.

User exec commands

Table 3 summarizes USER EXEC commands:

TABLE 3 User Exec Mode Command Summary

Command	Description	Ref.
clear	Resets the command to the previous configuration	*page 157*
clrscr	Clears the display screen	*page 32*
cluster-cli	Displays the cluster context	*page 159*
disable	Turns off (disables) the privileged mode command set	*page 160*
enable	Turns on (enables) the privileged mode command set	*page 161*
exit	Ends the current mode and moves down to the previous mode	*page 33*
help	Describes the interactive help system	*page 34*
logout	Exits the EXEC mode	*page 162*
no	Negates a command or sets its defaults	*page 35*
page	Toggles the paging functionality	*page 163*
ping	Sends ICMP echo messages	*page 164*
quit	Exits the current mode and moves to the previous mode	*page 165*
service	Displays service commands	*page 37*
show	Shows running system information. Refer to *Common commands on page 31*	*page 59*
telnet	Opens a telnet session	*page 166*

TABLE 3 User Exec Mode Command Summary

Command	Description	Ref.
terminal	Sets terminal line parameters	*page 167*
traceroute	Traces the route to a destination	*page 168*

clear

User exec commands

Resets the previous (last saved) command

Supported on the following platforms:

- Mobility RFS4000 Controller
- Mobility RFS6000 Controller
- Mobility RFS7000 Controller

NOTE
Refer to the interface details below when using clear counter interface.
- ge <index> – Mobility RFS4000 Controller supports 4 GEs and Mobility RFS6000 Controller supports 8 GEs
- me1 – Available in both Mobility RFS7000 Controller and Mobility RFS6000 Controller
- up1 – Available ib both Mobility RFS6000 Controller and Mobility RFS4000 Controller
- sa <1-4> – Available only in Mobility RFS7000 Controller
- sa <1-6> – Available only in Mobility RFS4000 Controller

Syntax

```
clear [crypto|mobility|spanning-tree]

clear crypto [ipsec|isakmp] sa {<IP>}

clear mobility [event-log|wireless-client|peer-statistics]
clear mobility event-log [wireless-client|peer]
clear mobility wireless-client [<MAC>|all|foreign-database|
       home-database]
clear mobility peer-statistics {<Peer-IP>}

clear spanning-tree detected-protocols {interface <interface-name>}
```

Parameters

crypto [ipsec|isakmp] sa *{<IP>}*	Clears IPSec/ISAKMP SAs for a given peer
	• ipsec sa *{<IP> }* – Clears IPSec SA's
	• isakmp sa *{<IP> }* – Clears ISAKMP SA's
	  • sa – Clears all IPSec/ISAKMP SA's
	  • <IP> – Optional. Peer IP address

mobility [event-log| wireless-client| peer-statistics]	Clears mobility attributes
	• event-log [wireless-client|peer]– Clears the event log
	  • wireless-client – Clears Client event-logs for
	  • peer – Clears peer event logs
	• wireless-client [<MAC>|all|foreign-database| home-database] – Clears Client information
	  • <MAC> – Clears the MAC addresses of a Client
	  • all – Clears the Client MAC address, including the foreign and home database
	  • foreign-database – Clears those clients present in the foreign Client database
	  • home-database – Clears those clients present in the home Client database
	• peer-statistics {<Peer-IP>} – Clears Mobility Peer Statistics
	  • <Peer-IP> – Optional. IP address of a Peer

spanning-tree detected-protocols *{interface <interface-name>}*	Clears the spanning tree protocols configured for the interface • detected-protocols {interface <interface-name>} – Enter the optional interface name <interface-name> to clear the detected spanning tree protocols for that specific interface

Example

```
RFController>clear crypto ike sa 111.222.333.01
RFController>
```

cluster-cli

User exec commands

Use this command to enter the cluster-cli context. The cluster-cli context provides centralized management to configure all cluster members from any one member. Any command executed under this context will be executed to all the controllers in the cluster.

A new context *redundancy* supports the cluster-cli. Any commands executed under this context are executed on all members of the cluster.

Supported in the following platforms:

- Mobility RFS4000 Controller
- Mobility RFS6000 Controller
- Mobility RFS7000 Controller

Syntax

```
cluster-cli enable
```

Parameters

enable	Enables the cluster context

Example

```
RFController> enable
RFController:cluster-cli>
```

disable

User exec commands

Enables the PRIV mode to use the disable command. Use the `disable` command to exit the PRIV mode

Supported in the following platforms:

- Mobility RFS4000 Controller
- Mobility RFS6000 Controller
- Mobility RFS7000 Controller

Syntax

```
disable
```

Parameters

None

Example

```
RFController>disable
RFController>
```

enable

User exec commands

Use the enable command to enter the PRIV mode

Supported in the following platforms:

- Mobility RFS4000 Controller
- Mobility RFS6000 Controller
- Mobility RFS7000 Controller

Syntax

```
enable
```

Parameters

None

Example

```
RFController>enable
RFController#
```

logout

User exec commands

Use this command instead of the `exit` command to exit the EXEC mode

Supported in the following platforms:

- Mobility RFS4000 Controller
- Mobility RFS6000 Controller
- Mobility RFS7000 Controller

Syntax

```
logout
```

Parameters

None

Example

```
The RFController Series Controller logs off on execution of this command.
```

page

User exec commands

Use the command to toggle the controller paging function. Enabling this command displays the CLI command output page by page, instead of running the entire output at once.

Supported in the following platforms:

- Mobility RFS4000 Controller
- Mobility RFS6000 Controller
- Mobility RFS7000 Controller

Syntax

```
page
```

Parameters

None

ping

User exec commands

Sends ICMP echo messages to a user-specified location

Supported in the following platforms:

- Mobility RFS4000 Controller
- Mobility RFS6000 Controller
- Mobility RFS7000 Controller

Syntax

```
ping {[<IP>|<hostname>]}
```

Parameters

ping *{[<IP>|<hostname>]}*	Pings the specified destination IP address or hostname. When entered without any parameters, this command prompts you for an IP/Host-name to ping.

Example

```
RFController>ping 192.168.2.100
PING 192.168.2.100 (192.168.2.100): 100 data bytes
128 bytes from 192.168.2.100: icmp_seq=0 ttl=128 time=2.7 ms
128 bytes from 192.168.2.100: icmp_seq=1 ttl=128 time=38.4 ms
128 bytes from 192.168.2.100: icmp_seq=2 ttl=128 time=4.6 ms

--- 192.168.2.100 ping statistics ---
3 packets transmitted, 3 packets received, 0% packet loss
round-trip min/avg/max = 2.7/15.2/38.4 ms
RFController>ping
Target IP address:
```

quit

User exec commands

Use this command to exit the current mode and move to the previous mode

Supported in the following platforms:

- Mobility RFS4000 Controller
- Mobility RFS6000 Controller
- Mobility RFS7000 Controller

Syntax

```
quit
```

Parameters

None

Example

The controller logs off upon execution of the command

telnet

User exec commands

Opens a telnet session

Supported in the following platforms:

- Mobility RFS4000 Controller
- Mobility RFS6000 Controller
- Mobility RFS7000 Controller

Syntax

```
telnet <IP> port
```

Parameters

telnet <IP> port	Defines the IP address or hostname of a remote system • port – Displays TCP port number

Example

```
Mobility RFS6000 Controller>telnet 172.16.10.3

Entering character mode
Escape character is '^]'.


Mobility RFS6000 Controller release 4.0.0.0-037D
Login as 'cli' to access CLI.
Mobility RFS6000 Controller login:
```

terminal

User exec commands

Sets the length/number of lines displayed within the terminal window

Supported in the following platforms:

- Mobility RFS4000 Controller
- Mobility RFS6000 Controller
- Mobility RFS7000 Controller

Syntax

```
terminal [length <0-512>|no [length <0-512>|width]|
       width <0-512>]
```

Parameters

length <0-512>	Sets the number of lines on a screen
no [length <0-512>| width]	Negates a command or sets its defaults. • length <0-512> – Negates the length command • width – Negates the width command
width <0-512>	Sets the width/number of characters on a screen line

Example

```
RFController>terminal length 100
RFController>

RFController>terminal width 200
RFController>
```

traceroute

User exec commands

Traces the route to its defined destination

Supported in the following platforms:

- Mobility RFS4000 Controller
- Mobility RFS6000 Controller
- Mobility RFS7000 Controller

Syntax

```
traceroute [[<IP>|<hostname>]|ip [<IP>|<hostname>]]
```

Parameters

[<IP>|<hostname>]	Traces the route to a destination IP address or a hostname
ip [<IP>|<hostname>]	IP trace to a destination IP address or a hostname

Example

```
RFController#traceroute 157.222.333.33
traceroute to 157.235.208.39 (157.235.208.39), 30 hops max, 38 byte packets
1 157.235.208.39 (157.235.208.39) 0.466 ms 0.363 ms 0.226 ms
RFController#
```

Chapter

4 Privileged Exec Commands

In this chapter

Most PRIV EXEC commands set operating parameters. Privileged-level access should be password protected to prevent unauthorized use. The PRIV EXEC command set includes commands contained within the USER EXEC mode. The PRIV EXEC mode also provides access to configuration modes, and includes advanced testing commands.

The PRIV EXEC mode prompt consists of the host name of the device followed by a pound sign (**#**). To access the PRIV EXEC mode, enter the following at the prompt:

```
RFController>enable
RFController#
```

The PRIV EXEC mode is often referred to as the *enable mode*, because the `enable` command is used to enter the mode. There is no provision to configure a password to get access to PRIV EXEC (enable) mode.

Priv Exec command

Table 4 summarizes the controller PRIV EXEC commands:.

TABLE 4 Priv Exec Commands

Command	Description	Ref.
acknowledge	Acknowledges alarms	*page 171*
archive	Manages archive files	*page 172*
cd	Changes the current directory	*page 174*
change-passwd	Changes the password of the logged user	*page 175*
clear	Resets controller functions to last saved configuration	*page 176*
clock	Configures the software system clock	*page 179*
clrscr	Clears the display screen	*page 32*
cluster-cli	Displays the cluster context	*page 180*
configure	Enters the configuration mode	*page 181*
copy	Copies content from one file to another	*page 182*
debug	Displays debugging functions	*page 183*
delete	Deletes a specified file from the system	*page 188*
diff	Displays differences between two files	*page 189*
dir	Lists the files on a filesystem	*page 190*
disable	Turns off privileged mode command	*page 191*

TABLE 4 Priv Exec Commands

Command	Description	Ref.
edit	Edits a text file	*page 192*
enable	Turns on the privileged mode command	*page 193*
erase	Erases a filesystem	*page 194*
exit	Ends the current mode and moves to the previous mode	*page 33*
halt	Halts the controller	*page 195*
help	Displays a description of the interactive help system	*page 34*
kill	Kills (terminates) a specified session	*page 196*
logout	Exits the EXEC mode	*page 197*
mkdir	Creates a directory	*page 198*
more	Displays the contents of a file	*page 199*
no	Negates a command or sets its defaults	*page 35*
page	Toggles the paging function	*page 201*
ping	Sends ICMP echo messages to a specified location	*page 202*
pwd	Displays the current directory	*page 203*
quit	Exits the current mode and moves to the previous mode	*page 204*
reload	Halts the controller and performs a warm reboot	*page 205*
rename	Renames a file	*page 206*
rmdir	Deletes a directory	*page 207*
service	Displays service commands	*page 37*
show	Shows running system information.	*page 59*
telnet	Opens a telnet session	*page 208*
terminal	Sets terminal line parameters	*page 209*
traceroute	Traces a route to a destination	*page 210*
upgrade	Upgrades the controller software image	*page 211*
upgrade - abort	Aborts an ongoing upgrade operation	*page 213*
write	Writes the running configuration to memory or a terminal	*page 214*

acknowledge

Priv Exec command

Acknowledges alarms

Supported in the following platforms:

- Mobility RFS4000 Controller
- Mobility RFS6000 Controller
- Mobility RFS7000 Controller

Syntax

```
acknowledge alarm-log [<1-65535>|all]
```

Parameters

alarm-log [<1-65535>|all]	Acknowledges alarms • <1-65535> – Acknowledges the specific alarm ID • all – Acknowledges all alarms

Example

```
RFController#acknowledge alarm-log all
No corresponding record found in the Alarm Log.

RFController#acknowledge alarm-log 200
No corresponding record found in the Alarm Log.
RFController#
```

archive

Priv Exec command

Manages file archive operations

Supported in the following platforms:

- Mobility RFS4000 Controller
- Mobility RFS6000 Controller
- Mobility RFS7000 Controller

Syntax

```
archive tar /table [<FILE>|<URL>]
archive tar /create [<FILE>|<URL>] [<FILE>|<DIR>]
archive tar /xtract [<FILE>|<URL>] <DIR>
```

Parameters

tar	Manipulates (creates, lists or extracts) a tar file
/table	Lists the files in a tar file
/create	Creates a tar file
/xtract	Extracts content from a tar file
<FILE>	Defines a Tar filename
<URL>	Tar file URL
<DIR>	A directory name. When used with /create, is the source directory for the tar file. When used with /xtract, is the destination file where the contents of the tar file are extracted to.

Example

How to zip the folder flash:/log/?

```
RFController#archive tar /create flash:/out.tar flash:/log/
tar: Removing leading '/' from member names
flash/log/
flash/log/snmpd.log
flash/log/messages.log
flash/log/startup.log
flash/log/radius/
RFController#dir flash:/
```

How to view the output tar file?

```
Directory of flash:/
  drwx   1024      Thu Apr 17 08:25:50 2010   hotspot
  drwx   120       Fri Apr  8 12:27:20 2010   log
  drwx   1024      Thu Apr  7 16:23:34 2010   crashinfo
  drwx   1024      Wed May 23 15:30:19 2010   backup
  -rw-   173056    Fri May  8 14:39:48 2010   out.tar
```

How to see which files are in the tar file?

```
RFController#archive tar /table flash:/out.tar
drwxrwxrwt 0/600  0 2010-05-08 12:27:20 flash/log
-rw-r--r-- 0/0    381 2010-05-08 12:27:28 flash/log/snmpd.log
-rw-r--r-- 0/0    151327 2010-05-08 14:37:26 flash/log/messages.log
```

```
-rw-r--r-- 0/0    17318 2010-05-08 12:27:29 flash/log/startup.log
drwxrwxrwt 0/600  0 2010-05-08 12:27:14 flash/log/radius
```

If Untar fails..?

```
RFController#archive tar /xtract flash:/out.tar flash:/out/
tar: flash:/out.tar: No such file or directory
```

cd

Priv Exec command

Changes the current directory

Supported in the following platforms:

- Mobility RFS4000 Controller
- Mobility RFS6000 Controller
- Mobility RFS7000 Controller

Syntax

```
cd {<DIR>}
```

Parameters

<DIR>	Changes current directory to DIR. This parameter is optional. When this parameter is not provided, the current directory name is displayed.

Example

```
RFController#cd
nvram:/   system:/  flash:/

RFController#cd flash:/?
  DIR  Change current directory to DIR

RFController#cd flash:/
flash:/backup/     flash:/crashinfo/  flash:/hotspot/    flash:/log/
flash:/out/

RFController#cd flash:/log/?
  DIR  Change current directory to DIR

RFController#cd flash:/log/
RFController#pwd
flash:/log/
RFController#
```

change-passwd

Priv Exec command

Changes the password of a logged user

Supported in the following platforms:

- Mobility RFS4000 Controller
- Mobility RFS6000 Controller
- Mobility RFS7000 Controller

Syntax

```
change-passwd
```

Parameters

None

Usage Guidelines

A password must be between 8 to 32 characters in length. For security, the console does not display user entered key words or the old password and new password fields.

Verify the console displays a “password successfully changed” message.

NOTE
The console (by default), does not display a user entered keyword for an old password and new password. Leaving the old password and new password fields empty displays the following error message: `Error: Invalid password length. It should be between 8 - 32characters.`

Example

```
RFController#change-passwd
Enter old password:
Enter new password:
Password for user 'admin' changed successfully
RFController#
```

clear

Priv Exec command

Resets the current context

Supported in the following platforms:

- Mobility RFS4000 Controller
- Mobility RFS6000 Controller
- Mobility RFS7000 Controller

Syntax

```
clear [aclstats|alarm-log|arp-cache|counters|crypto|
       dosstats|ip|logging|mac-address-table|mobility|
       spanning-tree]
clear [aclstats|arp-cache|dosstats|logging]

clear alarm-log [<1-65535>|acknowledge|all|new]

clear counters [all|bridge|firewall|igmp-snooping|interface|
       router|thread]
clear counters interface [<interface>|all|ge <1-8>|me1|sa <1-4>|up1|vlan
<1-4094>]
```

In the Mobility RFS4000 Controller:

```
clear counters interface [<interface>|all|ge <1-5>|me1|sa <1-6>|up1|vlan
<1-4094>|wwan]

clear crypto [ike|ipsec] sa {<IP>}

clear ip [dhcp|pmtu-discovery-blackhole-cache]
clear ip dhcp binding [*|<IP>|all]
clear ip pmtu-discovery-blackhole-cache

clear mac-address-table [dynamic|multicast|static]
       [address <address>|bridge <1-32>|interface <interface>|
       vlan <vlan>]

clear mobility [event-log|wireless-client|peer-statistics]
clear mobility event-log [wireless-client|peer]
clear mobility wireless-client [<MAC>|all|foreign-database|
       home-database]
clear mobility peer-statistics {<peer-IP>}

clear spanning-tree detected-protocols {interface <interface-name>}
```

Parameters

aclstats	Clears ACl statistics
alarm-log [<1-65535>|acknowledge|all|new]	Clears the alarm-log • <1-65535> – Clears the specific alarm ID • acknowledge – Clears acknowledged alarms • all – Clear all alarms • new – Clear new alarms
arp-cache	Clears the ARP cache
counters [all|bridge|firewall|igmp-snooping|interface|router|thread]	Clears counters • all – Clears all counters • bridge – Clears bridge counters • firewall – Clears firewall counters • interface [<interface>|all|ge <1-8>|me1|sa <1-4>|up1|vlan <1-4094>] – Clears interface counters • igmp-snooping – Clears igmp-snooping counters • router – Clears router counters • thread – Clear per-thread counters

crypto [ipsec|isakmp] sa *{<IP>}*	Clears IPSec/ISAKMP SAs for a given peer
	• ipsec sa {<IP> } – Clears IPSec SA's
	• isakmp sa {<IP> } – Clears ISAKMP SA's
	  • sa – Clears all IPSec/ISAKMP SA's
	  • <IP> – Optional. Peer IP address

ip [dhcp|pmtu-discovery-blackhole-cache]	Clears Internet Protocol (IP) DHCP/NAT
	• dhcp binding [*|<IP>|all]– DHCP server configuration
	  • binding [*|<IP>|all]– DHCP address bindings
	  • * – Clears all bindings
	  • <IP> – Clears a specific IP binding
	  • all – Clears
	• pmtu-discovery-blackhole-cache - Clears path
	For more details, see *DHCP Server Instance on page 507*

logging	Modifies message logging facilities

mac-address-table [dynamic|multicast|static] [address <address>|bridge <1-32>|interface <interface>|vlan <vlan>]	Clears entries in the forwarding database
	• dynamic – Clears all dynamic entries
	• multicast – Clears all multicast entries
	• static – Clears all management configured entries
	  • address <address> – Clears a specified MAC address
	  • bridge <1-32> – Clears bridge group commands
	  • interface <interface> – Clears all MAC addresses for the specified interface
	  • vlan <vlan> – Clears all MAD addresses for the specified VLAN (1-4094)

mobility [event-log| wireless-client| peer-statistics]	Clears mobility attributes
	• event-log [wireless-client|peer]– Clears the event log
	  • wireless-client – Clears Client event-logs for
	  • peer – Clears peer event logs
	• wireless-client [<MAC>|all|foreign-database home-database] – Clears Client information.
	  • <MAC> – Clears the MAC addresses of a Client
	  • all – Clears the Client MAC address, including the foreign and home database
	  • foreign-database – Clears those clients present in the foreign Client database
	  • home-database – Clears those clients present in the home Client database
	• peer-statistics {<peer-IP>}– Clears Mobility Peer Statistics
	  • <peer-IP> – IP address of a Peer

spanning-tree detected-protocols *{interface <interface-name>}*	Clears the spanning tree protocols configured for the interface • detected-protocols *{interface <interface-name>}* – Enter the optional interface name to clear the detected spanning tree protocols for that specific interface

Example

```
RFController#clear alarm-log new
RFController#
RFController#clear alarm-log acknowledged
RFController#
RFController#clear arp-cache
RFController#
RFController#clear logging
RFController#
RFController#clear mobility event-log peer
RFController#
RFController#clear ip dhcp binding *
RFController#
```

clock

Priv Exec command

Configures the software system clock

Supported in the following platforms:

- Mobility RFS4000 Controller
- Mobility RFS6000 Controller
- Mobility RFS7000 Controller

Syntax

```
clock set HH:MM:SS <1-31> <MONTH> <1993-2035>
```

Parameters

HH:MM:SS	Sets the time in hours, minutes, and seconds
<1-31>	Sets the number of days in the month.
<MONTH>	Sets the month in the format Jan, Feb, Mar,..., Dec.
<1993-2035>	Sets the year

Example

```
RFController#clock set 15:10:30 25 May 2010

RFController#show clock
May 25 15:10:31 UTC 2010
```

cluster-cli

Priv Exec command

Use this command to access the cluster-cli context. The cluster-cli context provides centralized management to configure all members of cluster from one member. Any command executed under this context is executed on all controllers in the cluster.

A new context (*redundancy*) is available to support the cluster-cli. Any commands executed under this context are executed on each cluster member.

Use `no cluster-cli` to exit the cluster-cli context.

Supported in the following platforms:

- Mobility RFS4000 Controller
- Mobility RFS6000 Controller
- Mobility RFS7000 Controller

Syntax

```
cluster-cli enable
```

Parameters

enable	Enables the controller cluster context

Example

```
RFController#cluster-cli enable
```

configure

Priv Exec command

Enters the configuration mode

Supported in the following platforms:

- Mobility RFS4000 Controller
- Mobility RFS6000 Controller
- Mobility RFS7000 Controller

Syntax

```
configure terminal
```

Parameters

terminal	Enables configuration from the terminal

Example

```
RFController#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
RFController(config)#
```

copy

Priv Exec command

Copies any file (config,log,txt ...etc) from any location to the controller and vice-versa

NOTE
Copying a new config file onto an existing running-config file merges it with the existing running-config on the controller. Both, the existing running-config and the new config file are applied as the current running-config.
Copying a new config file onto a start-up config files replaces the existing start-up config file with the parameters of the new file. It is better to erase the existing start-up config file and then copy the new config file to the startup config.

Supported in the following platforms:

- Mobility RFS4000 Controller
- Mobility RFS6000 Controller
- Mobility RFS7000 Controller

Syntax

```
copy [<FILE>|<URL>] [<FILE>|<URL>]
```

Parameters

<FILE>	The first <FILE> is the source file to copy from. The second <FILE> is the destination to which to copy.
<URL>	The first <URL> is the source URL to copy from. The second <URL> is the destination URL to which to copy.

Example

Transferring file snmpd.log to remote tftp server?

```
RFController#copy flash:/log/snmpd.log
tftp://157.235.208.105:/snmpd.log
```

Accessing running-config file from remote tftp server into controllerrunning-config?

```
RFController#copy tftp://157.235.208.105:/running-
config running-config
```

debug

Priv Exec command

Use this command for debugging

Supported in the following platforms:

- Mobility RFS4000 Controller
- Mobility RFS6000 Controller
- Mobility RFS7000 Controller

Syntax

```
debug [all|cc|ccstats|certmgr|dhcpsvr|imi|ip|logging|mgmt|
       mobility|mstp|nsm|radius|redundancy|rns|securitymgr|sole]
debug all
debug cc [access-point|all|alt|ap-containment|ap-detect|
       capwap|cluster|config|dot11|eap|ids|kerberos|l3-mob|
       loc-ap|loc-client|media|wireless-client|radio|radius|self-heal|
       smart|snmp|system|wips|wisp|wlan] {[debug|err|info|warn]}

debug ccstats <statsmodule>
debug [certmgr|dhcpsvr] [all|error|info]
debug imi [all|cli-client|cli-server|errors|init|ntp]
debug ip [https|ssh]
debug logging [all|errors|init|monitor|subagent]
debug mgmt [all|debug|err|info|sys|warning]
debug mobility [all|cc|error|forwarding|client|packet|peer|
       system]
debug mstp [all|cli|packet|protocol|timer]
debug nsm {[all|events|kernel|packet]}
debug radius {[all|err|info|warn]}
debug redundancy [all|ccmsg|config|errors|general|
       heartbeats|init|packets|proc|shutdown|states|subagent|
       timer|warnings]
debug securitymgr [acldebug|aclerror|all|debug|dosdebug|
       doserror|error|ikedebug|natdebug|naterror|
       packet-forwarding|pmdebug|pmerror|rulesdebug|
       ruleserror|user]
debug sole [adapters|aeroscout|algo|all|cclib|ekahau|errors|
       info|init]
```

Parameters

all	Enables debugging

cc [access-point|all|alt|ap-containment|apetect|capwap|cluster|config|dot11|eap|ids|kerberos|l3-mob|loc-ap|loc-client|media|wireless-client|radio|radius|self-heal|smart|snmp|system|wips|wisp|wlan] *{[debug|err|info|warn]}*	controller (wireless) debugging message
	• access-point [debug|err|info|warn] – Debugs access point logs
	  • debug – Debugs all default messages
	  • err – Debugs error and higher severity messages
	  • info – Debugs information and higher severity messages
	  • warn – Debugs warning and higher severity messages
	• all – all modules
	• alt [debug|err|info|warn] – address lookup logs
	• ap-detect [debug|err|info|warn] – rouge AP detection logs
	• ap-containment [debug|err|info|warn] – rouge AP containment logs
	• capwap [debug|err|info|warn] – capwap logs
	• cluster [debug|err|info|warn] – cluster related logs
	• config [debug|err|info|warn] – configuration change logs
	• dot11 [debug|err|info|warn] – data path logs
	• kerberos [debug|err|info|warn] – kerberos logs
	• l3-mob [debug|err|info|warn] – Layer3 mobility logs
	• loc-ap [debug|err|info|warn] – loc-ap logs
	• loc-client [debug|err|info|warn] – loc-client logs
	• media [debug|err|info|warn] – encapsulation media logs
	• wireless-client [debug|err|info|warn] – wireless client logs
	• radio [debug|err|info|warn] – radius logs
	• radius [debug|err|info|warn] – radius client logs
	• self-heal [debug|err|info|warn] – self healing logs
	• smart [debug|err|info|warn] – smart-rf logs
	• snmp [debug|err|info|warn] – SNMP logs
	• system [debug|err|info|warn] – system call logs
	• wips [debug|err|info|warn] – WIPS sensor logs
	• wisp [debug|err|info|warn] – wisp logs
	• wlan[debug|err|info|warn] – wlan logs

ccstats <stats-module>	Controller statistics (wireless) debugging messages
	• stats-module [debug|error|info|warn] – Statistics Module to be debugged.
	  • debug – Debugs all default messages
	  • err – Debugs error and higher severity messages
	  • info – Debugs information and higher severity messages
	  • warn – Debugs warning and higher severity messages

certmgr [all|error|info]	Certificate manager debugging messages • all – Trace error and informational messages from Certificate Manager • error – Trace error messages from Certificate Manager • info – Trace information messages from Certificate Manager
dhcpsvr [all|error|info]	DHCP Conf Server debugging messages • all – Trace error and informational messages from DHCP Conf Server • error – Trace error messages from DHCP Conf Server • info – Trace information messages from DHCP Conf Server

imi [all|cli-client| cli-server|errors|init|ntp]	Integrated management interface debugging messages • all – All debugging • cli-client – CLI responses from Protocol modules to IMI Server • cli-server – CLI commands from IMI server to protocol module • error – errors • init – Initialization process • ntp – Net debug messages
ip [https|ssh]	Internet protocol debugging messages • https – Secure HTTP <HTTPS> Server • ssh – Secure Shell <SSH> Server
logging [all|errors|init|monitor| subagent]	Modify message logging facilities for debugging messages • all – All debugging • error – errors • init – Logging module Initialization • monitor – Logging to monitors • sub-agent – Subagent
mgmt [all|debug|err|info|sys| warning]	Management daemon debugging messages • all – All debugging • debug – Debug • info – Info • sys – System • warning –Warning • error – errors
mobility [all|cc|error|forwarding| client|packet|peer|system]	L3 mobility debugging messages • all – All debugging <except “forwarding”> • cc – ccserver events • error – error • forwarding – Dataplane forwarding • client –Client events and state changes • packet – Control packets • peer – Peer establishment • system – System events

mstp
[all|cli|packet|protocol|
timer]
	Multiple Spanning Tree Protocol (MSTP) debugging message
	• all – all
	• cli – CLI commands
	• packet [rx|tx] – MSTP packets
	  • rx – receive packet
	  • tx – transmit packet
	• protocol detail – Protocol
	• timer detail – MSTP timers
	  • detail – Detailed output

nsm *{[all|events|kernel|packet]}*	*Network Service Module* (NSM) debugging messages. All parameters are optional.
	• all – Enable all debugging
	• events – NSM events
	• kernel – NSM kernel
	• packet [detail|recv|send] – NSM packets
	  • detail – Detailed information display
	  • recv [detail] – NSM receive packets
	  • detail – Detailed information display
	  • send [detail] – NSM send packets
	  • detail – Detailed information display

radius *{[all|err|info|warning]}*	RADIUS server debugging messages. All are optional parameters. • all – trace all messages from radius server • err– trace error messages from local radius server • info – trace error, warning and information messages from radius server • warn – trace error and warning messages from radius server
redundancy [all|ccmsg|config|errors|general|heartbeats|init|packets|proc|shutdown|states|subagent|timer|warnings]	Redundancy protocol debugging messages • all – Debugging all • ccmsg – Msg exchange with CC • config – Configuration processing • errors – Errors • general – General • heartbeats – Heartbeats processing • init – Redundancy initialization • packets – Packet processing • proc – Process flow • shutdown – Shutdown process • states – Redundancy states machine • subagent – Sub-agent • timer – Timer handlings • warning – Warnings

securitymgr [acldebug|aclerror|all|debug|dosdebug|doserror|error|ikedebug|natdebug|naterror|packet-forwarding|pmdebug|pmerror|rulesdebug|ruleserror|user]	Security manager debugging messages
	• acldebug – Trace debug messages from ACL module
	• aclerror – Trace error messages from ACL module
	• all – Trace all messages from Security Manager
	• debug – Trace general debug messages from Security Manager
	• dosdebug – Trace debug messages from DOS module
	• doserror – Trace error messages from DOS module
	• error – Trace general error messages from Security Manager
	• ikedebug – Trace debug messages from Ike
	• natdebug – Trace debug messages from NAT module
	• naterror – Trace error messages from NAT module
	• packet-forwarding <WORD> – Enable debug messages related to packet forwarding
	  • <WORD> – Module based debug string
	• pmdebug – Trace debug messages from Policy Manager API calls
	• pmerror – Trace error messages from Policy Manager API calls
	• rulesdebug – Trace debug messages from rules module
	• ruleserror – Trace error messages from debug module
	• user <WORD> – Enable debug messages from Policy manager library
	  • <WORD> – Module based debug string

sole [adapters|aeroscout|algo|all|cclib|ekahau|errors|info|init]	Location engine debugging messages • adapters – SOLE Adapter manager logs • aeroscout – Aeroscout logs • algo – Location algorithm logs • all – All module logs • cclib – cc library logs • errors – Error and higher severity logs • info – SOLE info logs • init – Initialization logs • ekahau – Ekahau logs

Example

```
RFController#debug ?
  all           Enable all debugging
  cc            Controller (wireless) debugging messages
  ccstats       Controller (wireless) debugging messages
  certmgr       Certificate Manager Debugging Messages
  dhcpsvr       DHCP Conf Server Debugging Messages
  imi           Integrated Management Interface
  ip            Internet Protocol (IP)
  logging       Modify message logging facilities
  mgmt          Mgmt daemon
  mobility      L3 Mobility
  mstp          Multiple Spanning Tree Protocol (MSTP)
  nsm           Network Service Module (NSM)
  pktdrvr       Pktdrvr (kernel wireless) debugging messages
  radius        RADIUS server debugging messages
  redundancy    Redundancy Protocol debugging messages
  securitymgr   Security Manager Debugging Messages
  sole          Location engine debugging messages
RFController#debug
```

delete

Priv Exec command

Deletes a specified file from the system

Supported in the following platforms:

- Mobility RFS4000 Controller
- Mobility RFS6000 Controller
- Mobility RFS7000 Controller

Syntax

```
delete [/force <FILE>|/recursive <FILE>|<FILE>]
```

Parameters

/force	Forces deletion without a prompt
/recursive	Performs a recursive delete
<FILE>	Specifies the filename(s) to be deleted

Example

```
RFController#delete flash:/out.tar flash:/out.tar.gz
Delete flash:/out.tar [y/n]? y
Delete flash:/out.tar.gz [y/n]? y

RFController#delete /force flash:/tmp.txt
RFController#

RFController#delete /recursive flash:/backup/
Delete flash:/backup//fileMgmt_350_180B.core

[y/n]? y
Delete

flash:/backup//fileMgmt_350_18212X.core_bk

[y/n]? n
Delete flash:/backup//imish_1087_18381X.core.gz

[y/n]? n
RFController#
```

diff

Priv Exec command

Displays the differences between 2 files

Supported in the following platforms:

- Mobility RFS4000 Controller
- Mobility RFS6000 Controller
- Mobility RFS7000 Controller

Syntax

```
diff [<FILE>|<URL>] [<FILE>|<URL>]
```

Parameters

<FILE>	The first <FILE> is the source file for the diff. The second <FILE> is the file to compare.
<URL>	The first <URL> is the source URL for the diff. The second <URL> is the URL to compare.

Example

```
RFController#diff startup-config running-config
--- startup-config
+++ running-config
@@ -89,7 +89,7 @@
  mobility peer 157.235.208.16
  wlan 1 enable
  wlan 1 ssid wlan123
- wlan 1 encryption-type wep128
+ wlan 1 encryption-type tkip
  wlan 1 authentication-type eap
  wlan 1 mobility enable
  wlan 1 radius server primary 127.0.0.1
@@ -184,10 +184,12 @@
  rad-user adam password 0 mypassword
  rad-user eve password 0 mypassword123
  rad-user sumi password 0 mypassword
+ rad-user test password 0 mypassword123
  rad-user vasavi password 0 mypassword123
  group kumar2
   rad-user sumi
-  policy wlan 2
+  policy vlan 44
+  policy wlan 10
    group kumar3
```

dir

Priv Exec command

View the list of files on a filesystem

Supported in the following platforms:

- Mobility RFS4000 Controller
- Mobility RFS6000 Controller
- Mobility RFS7000 Controller

Syntax

```
dir {[/all|/recursive] [<DIR>|all-filesystems]}
```

Parameters

/all	Lists all files
/recursive	Lists files recursively
<DIR>	Lists files in the named file path
all-filesystems	Lists the files on all filesystems

Example

```
RFController#dir
Directory of flash:/

  drwx   1024      Wed Jul 19 19:14:05 2010   hotspot
  drwx   120       Wed Aug 30 15:32:44 2010   log
  drwx   1024      Thu Aug 31 23:50:09 2010   crashinfo
  -rw-   14271     Tue Jul 25 15:16:41 2010   Radius-config
  -rw-   14271     Wed Jul 26 15:42:08 2010   flash:
  drwx   1024      Wed Aug  9 17:35:08 2010   radius
  -rw-   3426      Wed Jul 26 16:08:02 2010   running-config-new
  -rw-   13163     Wed Jul 26 16:08:42 2010   radius-config
  -rw-   80898     Thu Aug 17 14:59:39 2010   cli_commands.txt
  -rw-   65015     Fri Aug 11 19:57:37 2010   cli_commands.txtli_commands.txt
  -rw-   65154     Thu Aug 17 15:11:23 2010   cli_commands_180B.txt

RFController#
```

disable

Priv Exec command

Turns off the privileged mode command

Supported in the following platforms:

- Mobility RFS4000 Controller
- Mobility RFS6000 Controller
- Mobility RFS7000 Controller

Syntax

```
disable
```

Parameters

None

Example

```
RFController#disable
RFController>
```

edit

Priv Exec command

Edits a text file

Supported in the following platforms:

- Mobility RFS4000 Controller
- Mobility RFS6000 Controller
- Mobility RFS7000 Controller

Syntax

```
edit <FILE>
```

Parameters

<FILE>	Name of the file to be modified

Example

```
RFController#edit startup-config
GNU nano 1.2.4                                          startup-config

!
aaa authentication login default local none
service prompt crash-info
!
username admin password 1 8e67bb26b358e2ed20fe552ed6fb832f397a507d
username admin privilege  superuser
username operator password 1 fe96dd39756ac41b74283a9292652d366d73931f
!
!
!
spanning-tree mst configuration
 name My Name
!
no bridge multiple-spanning-tree enable bridge-forward
```

enable

Priv Exec command

Turns on the privileged mode command

Supported in the following platforms:

- Mobility RFS4000 Controller
- Mobility RFS6000 Controller
- Mobility RFS7000 Controller

Syntax

```
enable
```

Parameters

None

Example

```
RFController#enable
RFController#
```

erase

Priv Exec command

Erases a target filesystem

Supported in the following platforms:

- Mobility RFS4000 Controller
- Mobility RFS6000 Controller
- Mobility RFS7000 Controller

Syntax

```
erase [nvram:|flash:|startup-config|usb1:|usb2:|cf:]
```

Parameters

nvram:	Erases everything in nvram
flash:	Erases everything in flash
startup-config	Resets the configuration to factory default
usb1:	Erases everything in usb1
usb2:	Erases everything in usb2
cf:	Erases everything in cf

Example

```
RFController#erase startup-config
RFController#
```

halt

Priv Exec command

Stops (halts) the controller

Supported in the following platforms:

- Mobility RFS4000 Controller
- Mobility RFS6000 Controller
- Mobility RFS7000 Controller

Syntax

```
halt
```

Parameters

None

Example

```
RFController#halt
Wireless Controller will be halted, do you want to continue?
(y/n): y
Do you want to save current configuration? (y/n/d): y
[OK]
```

kill

Priv Exec command

Kills (terminates) a specified session and stops (halts) the controller

Supported in the following platforms:

- Mobility RFS4000 Controller
- Mobility RFS6000 Controller
- Mobility RFS7000 Controller

Syntax

```
kill session <1-16>
```

-

session	Active session (16 active sessions can be terminated)

Example

```
Telnet to controller
[xyz@xyz xyz]$ telnet

157.235.208.93
Trying 157.235.208.93...
Connected to 157.235.208.93 (157.235.208.93).
Escape character is '^]'.

RFController release 4.3.0.0
Login as 'cli' to access CLI.
login: root

RFController#show sessions
SESSION   USER       LOCATION        IDLE
  START TIME ** 1       root   Console           00:00m

Jan  1 00:00:00 1970    2    root   157.235.208.105   00:38m
Jan  1 00:00:00 1970    3    root   157.235.208.105   00:00m
Jan  1 00:00:00 1970

RFController#kill session 9
% Error: Invalid session number
RFController#kill session 3
~ # Connection closed by foreign host.
[xyz@xyz xyz]$
```

logout

Priv Exec command

Exits the EXEC mode and stops (halts) the controller

Supported in the following platforms:

- Mobility RFS4000 Controller
- Mobility RFS6000 Controller
- Mobility RFS7000 Controller

Syntax

```
logout
```

Parameters

None

Example

```
RFController#logout

RFController release 4.3.0.0
Login as 'cli' to access CLI.
RFController login:
```

mkdir

Priv Exec command

Creates a new directory in the filesystem

Supported in the following platforms:

- Mobility RFS4000 Controller
- Mobility RFS6000 Controller
- Mobility RFS7000 Controller

Syntax

```
mkdir <DIR>
```

Parameters

<DIR>	Directory name

Example

```
RFController#mkdir TestDIR
RFController#
```

more

Priv Exec command

Displays the contents of a file

Supported in the following platforms:

- Mobility RFS4000 Controller
- Mobility RFS6000 Controller
- Mobility RFS7000 Controller

Syntax

```
more <FILE>
```

Parameters

<FILE>	Displays the contents of the file

Example

```
RFController#more flash:/log/messages.log
Sep 08 12:27:30 2010: %PM-5-PROCSTOP: Process

"radiusd" has been stopped
Sep 08 12:27:31 2010: %LICMGR-6-NEWLICENSE:

Licensed AP count changed to 48
Sep 08 12:27:31 2010: %CC-5-COUNTRYCODE:

config: setting country code to [in:
India]
Sep 08 12:27:31 2010: %DAEMON-6-INFO: radiusd

[460]: Ready to process requests.
Sep 08 12:27:35 2010: %DAEMON-6-INFO: init:

Starting pid 328, console
/dev/ttyS0
Sep 08 12:27:37 2010: %AUTH-6-INFO: login[328]:

root login  on `ttyS0' from
`Console'
Sep 08 12:27:47 2010: %IMI-5-USERAUTHSUCCESS:

User 'admin' logged in with role
of ' superuser' from auth source 'local'
Sep 08 12:28:01 2010: %NSM-6-DHCPDEFRT: Default
route with gateway
157.235.208.246 learnt via DHCP
Sep 08 12:28:01 2010: %NSM-6-DHCPIP: Interface

vlan1 acquired IP address
157.235.208.93/24 via DHCP
Sep 08 12:29:07 2010: %CC-5-RADIOADOPTED: 11bg

radio on AP 00-A0-F8-BF-8A-A2
adopted
Sep 08 12:29:07 2010: %CC-5-RADIOADOPTED: 11a
```

```
radio on AP 00-A0-F8-BF-8A-A2
adopted
Sep 08 12:29:12 2010: %MOB-6-MUADD: Station 00

-0F-3D-E9-A6-54: Added to
Mobility Database
Sep 08 12:29:12 2010: %CC-6-STATIONASSOC:
```

page

Priv Exec command

Toggles controller paging. Enabling this command displays the command output page by page instead of running the entire output at once.

Supported in the following platforms:

- Mobility RFS4000 Controller
- Mobility RFS6000 Controller
- Mobility RFS7000 Controller

Syntax

```
page
```

Parameters

None

Example

```
RFController#page
RFController#
```

ping

Priv Exec command

Send (transmits) ICMP echo messages

Supported in the following platforms:

- Mobility RFS4000 Controller
- Mobility RFS6000 Controller
- Mobility RFS7000 Controller

Syntax

```
ping {<IP>}
```

Parameters

<IP>	Sets the ping destination address or hostname

Example

```
RFController#ping 157.235.208.39
PING 157.235.208.39 (157.235.208.39): 100 data bytes
128 bytes from 157.235.208.39: icmp_seq=0 ttl=64 time=2.3 ms
128 bytes from 157.235.208.39: icmp_seq=1 ttl=64 time=0.2 ms
128 bytes from 157.235.208.39: icmp_seq=2 ttl=64 time=0.3 ms
128 bytes from 157.235.208.39: icmp_seq=3 ttl=64 time=0.2 ms
128 bytes from 157.235.208.39: icmp_seq=4 ttl=64 time=0.1 ms
--- 157.235.208.39 ping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max = 0.1/0.6/2.3 ms
RFController#ping
Target IP address:
```

pwd

Priv Exec command

View the contents of the current directory

Supported in the following platforms:

- Mobility RFS4000 Controller
- Mobility RFS6000 Controller
- Mobility RFS7000 Controller

Syntax

```
pwd
```

Parameters

None

Example

```
RFController#pwd
flash:/
RFController#
```

quit

Priv Exec command

Exits the current mode and moves to the previous mode

Supported in the following platforms:

- Mobility RFS4000 Controller
- Mobility RFS6000 Controller
- Mobility RFS7000 Controller

Syntax

```
quit
```

Parameters

None

Example

```
RFController#quit

RFController release 4.3.0.0
Login as 'cli' to access CLI.
RFController login:
```

reload

Priv Exec command

Halts the controller and performs a warm reboot

Supported in the following platforms:

- Mobility RFS4000 Controller
- Mobility RFS6000 Controller
- Mobility RFS7000 Controller

Syntax

```
reload
```

Parameters

None

Example

```
RFController#reload
```

rename

Priv Exec command

Renames a file in the existing filesystem

Supported in the following platforms:

- Mobility RFS4000 Controller
- Mobility RFS6000 Controller
- Mobility RFS7000 Controller

Syntax

```
rename <FILE> <FILE>
```

Parameters

<FILE>	Specifies the file to rename. The first <FILE> is the old file name. The second <FILE> is the new file name.

Example

```
RFController#rename flash:/TestDIR/ NewTestDir
RFController#DIR
Directory of flash:/

  drwx   1024      Wed Jul 19 19:14:05 2010   hotspot
  drwx   120       Wed Aug 30 15:32:44 2010   log
  drwx   1024      Thu Aug 31 23:50:09 2010   crashinfo
  -rw-   14271     Tue Jul 25 15:16:41 2010   Radius-config
  -rw-   14271     Wed Jul 26 15:42:08 2010   flash:
  drwx   1024      Wed Aug  9 17:35:08 2010   radius
  -rw-   3426      Wed Jul 26 16:08:02 2010   running-config-new
  -rw-   13163     Wed Jul 26 16:08:42 2010   radius-config
  -rw-   80898     Thu Aug 17 14:59:39 2010   cli_commands.txt
  -rw-   65015     Fri Aug 11 19:57:37 2010   cli_commands.txtli_commands.txt
  -rw-   65154     Thu Aug 17 15:11:23 2010   cli_commands_180B.txt
  -rw-   32        Sat Sep  2 00:15:38 2010   cli_commands.save
  drwx   1024      Sat Sep  2 00:31:24 2010   NewTestDir

RFController#
```

rmdir

Priv Exec command

Deletes an existing file from the file system

Supported in the following platforms:

- Mobility RFS4000 Controller
- Mobility RFS6000 Controller
- Mobility RFS7000 Controller

Syntax

```
rmdir <DIR>
```

Parameters

<DIR>	Defines the name of the directory to delete

Example

```
RFController#rmdir flash:/NewTestDir/
RFController#DIR
Directory of flash:/

  drwx   1024      Wed Jul 19 19:14:05 2010   hotspot
  drwx   120       Wed Aug 30 15:32:44 2010   log
  drwx   1024      Thu Aug 31 23:50:09 2010   crashinfo
  -rw-   14271     Tue Jul 25 15:16:41 2010   Radius-config
  -rw-   14271     Wed Jul 26 15:42:08 2010   flash:
  drwx   1024      Wed Aug  9 17:35:08 2010   radius
  -rw-   3426      Wed Jul 26 16:08:02 2010   running-config-new
  -rw-   13163     Wed Jul 26 16:08:42 2010   radius-config
  -rw-   80898     Thu Aug 17 14:59:39 2010   cli_commands.txt
  -rw-   65015     Fri Aug 11 19:57:37 2010   cli_commands.txtli_commands.txt
  -rw-   65154     Thu Aug 17 15:11:23 2010   cli_commands_180B.txt
  -rw-   32        Sat Sep  2 00:15:38 2010   cli_commands.save
```

telnet

Priv Exec command

Opens a telnet session

Supported in the following platforms:

- Mobility RFS4000 Controller
- Mobility RFS6000 Controller
- Mobility RFS7000 Controller

Syntax

```
telnet <IP> {<port>}
```

Parameters

telnet <IP> *{<port>}*	Defines the IP address or hostname of a remote system • <port> - Optional. Displays TCP Port Number

Example

```
RFController#telnet 157.111.222.33

Entering character mode
Escape character is '^]'.

Red Hat Linux release 9 (Shrike)
Kernel 2.4.20-6bigmem on an i686
login: cli
Password:
```

terminal

Priv Exec command

Sets the length/number of lines displayed within the terminal window

Supported in the following platforms:

- Mobility RFS4000 Controller
- Mobility RFS6000 Controller
- Mobility RFS7000 Controller

Syntax

```
terminal [length <0-512>|no [length <0-512>|width]|
       width <0-512>]
```

Parameters

length <0-512>	Sets the number of lines on a screen • <0-512> – Number of lines on a screen
no [length <0-512>| width]	Negates a command or sets its defaults • length <0-512> – Unset number of lines on a screen • width – Set width of display terminal
width <0-512>	Sets the width/number of characters on a screen line • <0-512> – Number of characters on a screen

Example

```
RFController>terminal length 100
RFController>

RFController>terminal width 200
```
RFController>

traceroute

Priv Exec command

Traces a route to a destination

Supported in the following platforms:

- Mobility RFS4000 Controller
- Mobility RFS6000 Controller
- Mobility RFS7000 Controller

Syntax

```
traceroute [[<IP>|<hostname>]|ip [<IP>|<hostname>]]
```

Parameters

[<IP>|<hostname>]	Traces the route to a destination IP address or a hostname
ip [<IP>|<hostname>]	IP trace to a destination IP address or a hostname

Example

```
RFController#traceroute 157.222.333.33
traceroute to 157.235.208.39 (157.235.208.39), 30 hops max, 38 byte packets
 1  157.235.208.39 (157.235.208.39)  0.466 ms  0.363 ms  0.226 ms
RFController#
```

upgrade

Priv Exec command

Upgrades the software image

Supported in the following platforms:

- Mobility RFS4000 Controller
- Mobility RFS6000 Controller
- Mobility RFS7000 Controller

Syntax

```
upgrade <URL> {background}
```

Parameters

<URL>	Location of the target firmware image used in upgrade
background	Optional. Specifies that the upgrade should occur in the background.

Example

```
RFController#upgrade tftp://157.235.208.105:/img
var2 is 10 percent full
/tmp is 2 percent full
Free Memory 161896 kB
FWU invoked via Linux shell
Running from partition /dev/hda5, partition to

update is /dev/hda6
Reading image file header
Removing other partition
Sep 08 15:57:18 2010: %KERN-6-INFO: EXT3 FS on

hda1, internal journal.
Making file system
Extracting files (this can take some time).Sep
.........................
Jan 08 15:58:17 2009: %DIAG-4-CPULOAD: One
minute average load limit exceeded,
value is 100.00% limit is 99.90% (top process
kernel/ISR 100.00%)
Sep 08 15:58:44 2009: %PM-4-PROCNORESP: Process

"logd" is not responding
Jan 08 15:58:44 2009: %PM-4-PROCNORESP: Process

"logd" is not responding
Jan08 15:58:44 2009: %PM-4-PROCNORESP: Process
"logd" is not responding
Jan 08 15:58:44 2009: %PM-4-PROCNORESP: Process

"logd" is not responding
Version of firmware update file is 4.3.0.0
19193X
Jan08 15:58:44 2009: %KERN-6-INFO: EXT3 FS on
```

```
hda1, internal journal.
Creating LILO files
Running LILO
Successful
Jan 08 15:58:46 2009: %FWU-6-FWUDONE: Firmware

update successful, new version is 4.3.0.0
RFController#
```

upgrade - abort

Priv Exec command

Aborts an ongoing upgrade process

Supported in the following platforms:

- Mobility RFS4000 Controller
- Mobility RFS6000 Controller
- Mobility RFS7000 Controller

Syntax

```
upgrade-abort
```

Parameters

None

Example

RFController#upgrade-abort

write

Priv Exec command

Writes the running configuration to memory or a terminal

Supported in the following platforms:

- Mobility RFS4000 Controller
- Mobility RFS6000 Controller
- Mobility RFS7000 Controller

Syntax

```
write [memory|terminal]
```

Parameters

memory	Writes to NV memory
terminal	Writes to terminal

Example

```
RFController#write terminal
!
! configuration of RFController version 4.3.0.0
version 1.0
!
service prompt crash-info
!
username admin password 1 8e67bb26b358e2ed20fe552ed6fb832f397a507d
username admin privilege  superuser
username operator password 1 fe96dd39756ac41b74283a9292652d366d73931f
username manager password 1 45b27d6483fc630981ad5096ff26a7956ce0c038
username manager privilege  superuser
!
!no country-code
logging console 7
no logging on
fallback enable
ftp password 1 810a25d76c31e495cc070bdf42e076f7c9b0a1cd
ip http server
ip http secure-trustpoint local
ip http secure-server
ip ssh
ip telnet
snmp-server manager v2
snmp-server manager v3
crypto isakmp identity address
crypto isakmp keepalive 10
crypto ipsec security-association lifetime kilobytes 4608000
!.....................................
```

format

Priv Exec command

Formats file system

Supported in the following platforms:

- Mobility RFS7000 Controller

NOTE
This command is not supported on the Mobility RFS4000 Controller and on the Mobility RFS6000 Controller.

Syntax

```
format cf:
```

Parameters

cf:	Formats compact flash

Example

```
RFController#format cf:
```

Chapter

Global Configuration Commands

5

In this chapter

The term global is used to indicate characteristics or features effecting the system as a whole. Use the Global Configuration Mode to configure the system globally, or enter specific configuration modes to configure specific elements (such as interfaces or protocols). Use the configure terminal command (under PRIV EXEC) to enter the global configuration mode.

The example below describes the process of entering the global configuration mode from privileged EXEC mode:

```
RFController# configure terminal
RFController(config)#
```

NOTE
The system prompt changes to indicate you are now in global configuration mode. The prompt for global configuration mode consists of the device host name followed by (config) and the pound sign (#).

Commands entered in the global configuration mode update the running configuration file as soon as they are entered. However, these changes are not saved in the startup configuration file until a *copy running-config startup-config* EXEC command is issued.

Global Configuration commands

Table 5 summarizes the Global Config commands

TABLE 5 Global Config Commands

Command	Description	Ref.
aaa	Configures the current authentication, authorization and accounting (aaa) login settings	*page 220*
access-list	Adds an access list entry	*page 221*
autoinstall	Autoinstalls a configuration command	*page 226*
banner	Defines a login banner	*page 228*
boot	Reboots the controller	*page 229*
bridge	Displays bridge group commands	*page 230*
clrscr	Clears the display screen	*page 32*
country-code	Configures the country of operation. All existing radio configuration will be erased	*page 232*
crypto	Defines encryption parameters	*page 233*

TABLE 5 Global Config Commands

Command	Description	Ref.
do	Runs commands from the EXEC mode	*page 245*
end	Ends the current mode and moves to the EXEC mode	*page 246*
errdisable	Recovers from errors	*page 247*
exit	Ends the current mode and moves to the previous mode	*page 33*
ftp	Configures FTP server parameters	*page 248*
help	Describes the interactive help system	*page 34*
hostname	Sets the system's network name	*page 249*
interface	Defines an interface to configure	*page 250*
ip	Internet Protocol (IP)	*page 252*
license	Sets license management commands	*page 259*
line	Configures a terminal line	*page 260*
local	Sets the username and password for local user authentication	*page 261*
logging	Modifies message logging facilities	*page 262*
mac	Configures MAC access-lists	*page 265*
mac-address-table	Configures MAC address table	*page 266*
mac-name	Sets a name to the MAC address of a Client	*page 267*
management	Sets properties of the management interface	*page 268*
no	Negates a command or set its defaults	*page 35*
ntp	Configures *Network Time Protocol* (NTP) parameters	*page 269*
prompt	Sets the system prompt	*page 273*
radius-server	Enters the RADIUS server mode	*page 274*
ratelimit	Sets the rate limit feature parameters	*page 275*
redundancy	Configures redundancy group parameters	*page 276*
role	Sets the Role Based Firewall parameters	*page 278*
rtls	Configures Real Time Location System parameters	*page 280*
show	Displays the running system information	*page 59*
service	Service commands	*page 281*
smtp-notification	Modifies SMTP notification parameters	*page 284*
snmp-server	Modifies SNMP engine parameters	*page 291*
spanning-tree	Configures spanning tree commands	*page 301*
timezone	Configures the timezone	*page 304*
traffic-shape	Configures traffic shaping	*page 305*
username	Establishes user name authentication	*page 308*
vpn	Defines the VPN configuration	*page 310*
wireless	Configures wireless parameters	*page 311*

TABLE 5 Global Config Commands

Command	Description	Ref.
wlan-acl	Applies an ACL on WLAN	*page 312*
network-element-id	Sets system's network element ID	*page 315*
firewall	Configures Wireless firewall	*page 316*
virtual-ip	Displays virtual-ip configuration details	*page 318*
wwan	Displays wireless wwan interface	*page 320*
aap-wlan-acl	Applies an acl on wlan for aap	*page 321*
arp	Configures Address Resolution Protocol	*page 322*
power	Configures PoE command	*page 323*
aap-ipfilter-list	Applies ipfilter to WLAN/LAN	*page 324*
whitelist	Configures host whitelist	*page 325*

aaa

Global Configuration commands

Configures the current *Authentication, Authorization and Accounting* (AAA) login settings

Supported in the following platforms:

- Mobility RFS4000 Controller
- Mobility RFS6000 Controller
- Mobility RFS7000 Controller

Syntax

```
aaa [authentication|nas|vpn-authentication]

aaa authentication login default [local|none|radius]
aaa nas <name>
aaa vpn-authentication [primary|secondary] <IP> key [0 <secret>|2
<secret>|<secret>] {authport <1024-65535>}
```

Parameters

authentication login default [local|none|radius]	Sets the authentication configuration parameters.
	• login – Sets the authentication lists for login
	• default – Defines the default authentication list
	  • local – Sets the local user database
	  • none – No authentication
	  • radius – Defines an external RADIUS server

nas <name>	Sets the NAS identifier. The <name> parameter accepts a string of 64 characters.

vpn-authentication [primary|secondary] [<IP> key [0 <secret>| 2 <secret>|<secret>] *{authport <1024-65535>}*	Sets the configuration for VPN authentication using RADIUS.
	• primary – Sets the configuration for the primary server
	• secondary – Sets the configuration for the secondary server
	• key [0 <secret>|2 <secret>|<secret>] – Sets the secret key settings
	  • 0 <secret> – Indicates that the password is specified unencrypted
	  • 2 <secret> – Indicates that the password is encrypted with password-encryption secret
	  • <secret> – A shared secret up to 32 characters
	• authport <1024-65535> – Sets an optional RADIUS Server authentication port

Usage Guidelines

Use an AAA login to determine whether management user authentication must be performed against a local user database or an external RADIUS server

access-list

Global Configuration commands

Adds an *Access List* (ACL) entry. Use the `access-list` command (under Global Configuration) to configure the access list mechanism for filtering frames by protocol type or vendor code.

ACLs control access to the network through a set of rules. Each rule specifies an action which is taken when a packet matches it within the given set of rules. If the action is *deny*, the packet is dropped and if the action is *permit*, the packet is allowed. The controller supports the following ACLs:

- IP Standard ACLs
- IP Extended ACLs
- MAC Extended ACLs

ACLs are identified by either a number or a name. Numbers are predefined for IP Standard and Extended ACLs, and the name can be any valid alphanumeric string (not exceeding 64 characters). With numbered ACLs, the rule parameters have to be specified on the same command line along with the ACL identifier.

Supported in the following platforms:

- Mobility RFS4000 Controller
- Mobility RFS6000 Controller
- Mobility RFS7000 Controller

Syntax

```
access-list [<1-99>|<100-199>|<1300-1999>|<2000-2699>]
```

For Standard IP ACLs:

```
access-list [<1-99>|<1300-1999>] [deny|permit|mark]
access-list [<1-99>|<1300-1999>] deny [<IP/MASK>|any|
       host <IP>] {[rule-precedence <1-5000>|
       log {rule-precedence <1-5000>}]}
access-list [<1-99>|<1300-1999>] permit [<IP/MASK>|any|
       host <IP>] {[rule-precedence <1-5000>|
       log {rule-precedence <1-5000>}]}
access-list [<1-99>|<1300-1999>] mark [8021p <0-7>|
dscp <0-63>|tos <0-255>] [<IP/MASK>|any|host <IP>]
{[rule-precedence <1-5000>|log {rule-precedence <1-5000>}]}
```

For Extended IP ACLs:

```
access-list [<100-199>|<2000-2699>] [deny|permit|mark] [icmp|ip|tcp|upd]

access-list [<100-199>|<2000-2699>] [deny|permit|mark] icmp
[<source-IP/Mask>|any|host <IP>] [<dest-IP/Mask>|any|host <IP>] {<ICMP-type>
{<ICMP-code>}} {log} {rule-precedence <1-5000>}

access-list [<100-199>|<2000-2699>] [deny|permit|mark]ip
[<source-IP/Mask>|any|host <IP>] [<dest-IP/Mask>|any|host <IP>] {log}
{rule-precedence <1-5000>}
```

```
access-list [<100-199>|<2000-2699>] [deny|permit|mark] [tcp|udp]
[<source-IP/Mask>|any|host <IP>] {eq
<source-port>|range <starting-source-port>
<ending-source-port>} [<dest-IP/Mask|any|host <IP>]
{eq <source-port>} {range <starting-source-port>
<ending-source-port>} {log} {rule-precedence <1-5000>}
```

NOTE

Using `access-list [<100-199>|<2000-2699>]` moves you to the **`(config-ext-nacl)`** instance. For additional information, see *Extended ACL Instance on page 449*.

Using `access-list [<1-99>|<1300-1999>]` moves you to the **`(config-std-nacl)`** instance. For additional information, see *Standard ACL Instance on page 471*.

To create a named ACL, use `ip access-list` (Standard/Extended). For more information, see *ip on page 252*.

Parameters

access-list [<1-99>|<1300-1999>] [permit|deny] [<IP/MASK>|any| host <IP>] *{[rule-precedence <1-5000> {log}|log]}*	Adds a standard access list entry. • [<1-99>|<1300-1999>] – Defines access list number from 1-99 or 1300-1999 • [deny|permit] – Defines action types on an ACL • [<IP/MASK>| host <IP>| any] – <IP/MASK> is the source address of the network or host in dotted decimal format For example, 101110/24 indicates the first 24 bits of the source IP are used for matching • The keyword **any** is an abbreviation for a source IP of 0.0.0.0 and source-mask bits equal to 0 • The keyword **host** is an abbreviation for exact source (A.B.C.D) and source-mask bits equal to 32 • log – Generates log messages when the packet coming from the interface matches the ACL entry. Log messages are generated only for router ACL's. This is an optional parameter • rule-precedence <1-5000> – Define an Integer value between 1-5000. This value sets the rule precedence in the ACL. This is an optional parameter
access-list [<1-99>|<1300-1999>] mark [8021p <0-7>|dscp <0-63>|tos <0-255>] [<IP/MASK>|any|host <IP>] *{[rule-precedence <1-5000> {log}|log]}*	Adds a standard access list entry. • [<1-99>|<1300-1999>] – Defines access list number from 1-99 or 1300-1999 • mark – Marks a packet. The action type **`mark`** is functional only over a Port ACL • 8021p <0-7> – Used only with the action type `mark` to specify 8021p priority values • dscp <0-63> – Used only with the action type `mark` to specify DSCP values • tos <0-255> – Used only with the action type `mark` to specify *type of service* (tos) values • [<IP/MASK>| host <IP>| any] – <IP/MASK> is the source address of the network or host in dotted decimal format. For example, 10.1.1.10/24 indicates the first 24 bits of the source IP are used for matching • The keyword **any** is an abbreviation for a source IP of 0.0.0.0 and source-mask bits equal to 0 • The keyword **host** is an abbreviation for exact source (A.B.C.D) and source-mask bits equal to 32 • log – Generates log messages when the packet coming from the interface matches the ACL entry. Log messages are generated only for router ACL's. This is an optional parameter • rule-precedence <1-5000> – Define an Integer value between 1-5000. This value sets the rule precedence in the ACL. This is an optional parameter

access-list [<100-199>|<2000-2699>] [permit|deny] [icmp|ip|tcp|udp] [<IP/MASK>|any| host <IP>] *{[rule-precedence <1-5000> {log}|log]}*	Adds an Extended IP access list entry.
	• (<100-199>|<2000-2699>) – For ICMP extended ACLs, the ACL must be between 2000-2699
	  • [deny|permit] – Defines action types on an ACL
	  • [icmp|ip|tcp|udp] – The protocol type for the extended ACL entry
	  • [<IP/MASK>| host <IP>| any] – <IP/MASK> is the source address of the network or host in dotted decimal format. For example, 10.1.1.10/24 indicates the first 24 bits of the source IP are used for matching
	  • The keyword **any** is an abbreviation for a source IP of 0.0.0.0 and source-mask bits equal to 0
	  • The keyword **host** is an abbreviation for exact source (A.B.C.D) and source-mask bits equal to 32
	  • log – Generates log messages when the packet coming from the interface matches the ACL entry. Log messages are generated only for router ACL's. This is an optional parameter
	  • rule-precedence <1-5000> – Define an Integer value between 1-5000. This value sets the rule precedence in the ACL. This is an optional parameter

access-list [<100-199>|<2000-2699>] mask [8021p <0-7>|dscp <0-63>|tos <0-255>] [icmp|ip|tcp|udp] [<IP/MASK>|any| host <IP>] *{[rule-precedence <1-5000> {log}|log]}*	Adds an Extended IP access list entry.
	• (<100-199>|<2000-2699>) – For ICMP extended ACLs, the ACL must be between 2000-2699
	  • mark – Marks a packet. The action type `mark` is functional only over a Port ACL
	  • 8021p <0-7> – Used only with the action type `mark` to specify 8021p priority values
	  • dscp <0-63> – Used only with the action type `mark` to specify DSCP values
	  • tos <0-255> – Used only with the action type `mark` to specify *type of service* (tos) values
	  • [icmp|ip|tcp|udp] – The protocol type for the extended ACL entry
	  • [<IP/MASK>| host <IP>| any] – <IP/MASK> is the source address of the network or host in dotted decimal format. For example, 10.1.1.10/24 indicates the first 24 bits of the source IP are used for matching
	  • The keyword **any** is an abbreviation for a source IP of 0.0.0.0 and source-mask bits equal to 0
	  • The keyword **host** is an abbreviation for exact source (A.B.C.D) and source-mask bits equal to 32
	  • log – Generates log messages when the packet coming from the interface matches the ACL entry. Log messages are generated only for router ACL's. This is an optional parameter
	  • rule-precedence <1-5000> – Define an Integer value between 1-5000. This value sets the rule precedence in the ACL. This is an optional parameter

Use an access list command under the global configuration to create an access list. The controller supports port, router and WLAN ACLs

- When the access list is applied on an Ethernet port, it becomes a port ACL
- When the access list is applied on a VLAN interface, it becomes a router ACL
- When the access list is applied on a WLAN index, it becomes a WLAN ACL

A MAC access list (to allow arp), is mandatory for both port and WLAN ACL's. For more information on how to configure a MAC access list, see *permit on page 499*.

Example

The example below creates a standard access list (ACL) to permit any traffic coming to the interface:

```
RFController(config)#access-list 1 permit any
RFController(config)#
```

The example below creates a extended IP access list to permit IP traffic between two networks:

```
RFController(config)#access-list 101 permit ip 192.168.1.0/24 192.168.2.0/24

RFController(config)#
```

The example below creates a extended access list to permit tcp traffic, between two networks, with destination port range between 20 and 23:

```
RFController(config)#access-list 101 permit tcp 192.168.1.0/24 192.168.2.0/24
range 20 23
RFController(config)#
```

The example below denies icmp traffic from any source to any destination:

```
RFController(config)#access-list 115 deny icmp any any
RFController(config)#access-list 115 permit ip any any
RFController(config)#
```

autoinstall

Global Configuration commands

Autoinstalls the controller image

Supported in the following platforms:

- Mobility RFS4000 Controller
- Mobility RFS6000 Controller
- Mobility RFS7000 Controller

Syntax

```
autoinstall [clear-config-history|cluster-config|config|
       image|reset-config|start]
autoinstall [clear-config-history|reset-config|start]
autoinstall [cluster-config|config] {url <URL>}
autoinstall image {[url <URL>|version <version>]}
```

Parameters

clear-config-history	Autoinstalls a clear configuration history, resulting in a reversion.
cluster-config *{url <URL>}*	Autoinstalls a cluster-config setup. • url – Optional. Sets the URL of the item • <URL> – Remote/external location of the file URLS: tftp://<hostname|IP>[:port]/path/file ftp://<user>:<passwd>@<hostname|IP>[:port]/path/file http://<hostname|IP>[:port]/path/file cf:/path/file usb1:/path/file usb2:/path/file
config *{url <URL>}*	Autoinstalls a config setup. • url – Optional. Sets the URL of the item • URL – Remote/external location of the file URLS: tftp://<hostname|IP>[:port]/path/file ftp://<user>:<passwd>@<hostname|IP>[:port]/path/file http://<hostname|IP>[:port]/path/file cf:/path/file usb1:/path/file usb2:/path/file
image *{[url <URL>| version <version>]}*	Autoinstalls the image setup. • url – Optional. Sets the URL of the item • <URL> – Remote/external location of the file URLS: tftp://<hostname|IP>[:port]/path/file ftp://<user>:<passwd>@<hostname|IP>[:port]/path/file http://<hostname|IP>[:port]/path/file cf:/path/file usb1:/path/file usb2:/path/file • version <version> – The version number <version> cannot be the same as the currently installed version number. Attempting to install the same version results in an unsuccessful download
reset-config	Resets all autoinstall features to factory defaults
start	Starts the autoinstall sequence

Example

```
RFController(config)#autoinstall clear-config-history
RFController(config)#
```

banner

Global Configuration commands

Defines a login banner for the controller. Use `{no} banner` to delete a previously configured banner.

Supported in the following platforms:

- Mobility RFS4000 Controller
- Mobility RFS6000 Controller
- Mobility RFS7000 Controller

Syntax

```
{no} banner motd [<message>|default]
```

Parameters

motd [<message>| default]	Sets the *message of the day* (MOTD) banner. <message> is the custom message to be displayed.Use default to set the MOTD string to the default message for the controller.

Usage Guidelines

Use **`no banner motd`** to delete the previously configured banner.

Example

```
RFController(config)#banner motd Welcome to my RFController CLI
RFController(config)

RFController release 4.3.0.0
Login as 'cli' to access CLI.
RFController login: cli
Welcome to my RFController CLI
Welcome to my RFController CLI
RFController>

RFController release 4.3.0.0
Login as 'cli' to access CLI.
RFController login: cli
Welcome to CLI
Welcome to CLI

RFController>
```

boot

Global Configuration commands

Reboots the controller with an image in the mentioned partition (either the primary or secondary partition)

Supported in the following platforms:

- Mobility RFS4000 Controller
- Mobility RFS6000 Controller
- Mobility RFS7000 Controller

Syntax

```
boot system [primary|secondary]
```

Parameters

system [primary|secondary]	Specifies the boot image used after reboot • primary – Specifies the primary image • secondary – Specifies the secondary image

Example

```
RFController(config)#boot system primary
Wireless controller will be rebooted, do you want to continue? (y/n):y
Do you want to save the configuration? (y/n):y

The system is going down NOW !!

% Connection is closed by administrator!
Please stand by while rebooting the system.
```

bridge

Global Configuration commands

Configures bridge specific commands

Supported in the following platforms:

- Mobility RFS4000 Controller
- Mobility RFS6000 Controller
- Mobility RFS7000 Controller

NOTE
The interfaces mentioned below are supported in the following platforms:
- ge <index> – Mobility RFS4000 Controller and Mobility RFS4000 Controller support 4 GEs and Mobility RFS6000 Controller supports 8 GEs
- sa <1-4> – Supported on Mobility RFS7000 Controller
- sa <1-6> – Supported on Mobility RFS4000 Controller
- me1 – Only supported on Mobility RFS6000 Controller and Mobility RFS6000 Controller
- up1 – Only supported on Mobility RFS6000 Controller and Mobility RFS4000 Controller

Syntax

```
{no} bridge [<bridgegroup>|multiple-spanning-tree]

bridge <bridegegroup> [address|ageing-time]
bridge  <bridegegroup> address <MAC> [discard|forward] [<interface>|ge
<1-8>|me1|sa <1-4>|up1|vlan <1-4094>]
bridge <bridegegroup> ageing-time [0|<10-1000000>]

bridge multiple-spanning-tree enable
```

Parameters

bridge <bridge-group> address <MAC> [discard|forward] [<interface>|ge <1-8>| me1|sa <1-4>|up1| vlan <1-4094>]
bridge <bridge-group> ageing-time [0|<10-1000000>]
	Bridge groups available for bridging.
	• <bridgegroup> – Bridge group value between 1 and 32
	• address <MAC> – Unique hardware address in the HHHH.HHHH.HHHH format
	  • [discard|forward] – Either discard or forward the interface on which the configured rule is applied. This filter frames on a specific interface that contain the specified hardware address in either the source or destination field
	  • <interface> – The name of the interface
	  • vlan <2-4094> – VLAN interface
	  • ge <index> – Gigabit Ethernet interface. Mobility RFS7000 Controller supports 4 GE's and Mobility RFS6000 Controller supports 8 GEs
	  • sa <1-4> – Static Aggregate interface index. Only supported on Mobility RFS7000 Controller
	  • me1 – Fast Ethernet interface
	  • up1 – WAN interface. Only available on Mobility RFS6000 Controller and Mobility RFS4000 Controller
	• ageing-time [0|<10-1000000>] – The time duration a learned MAC address persists after the last update
	  • 0 – Disables aging
	  • <10-1000000> – Sets aging time in seconds

multiple-spanning-tree enable	Enables *Multiple Spanning Tree Protocol* (MSTP) commands

Usage Guidelines

Creating customized filter schemes for bridged networks limits the amount of unnecessary traffic processed and distributed by the bridging equipment. Use multiple bridge address discard/forward commands to develop the filter scheme.

Use the `(no)bridge [<1-32>|multiple-spanning-tree]`command to delete the configured discard or forward filters.

Example

```
RFController(config)#bridge multiple-spanning-tree enable
RFController(config)#

RFController(config)#bridge 2 address 1a2b:3c4d:5e6f forward eth 1 vlan 2
RFController(config)#
```

country-code

Global Configuration commands

Sets the country of operation

Supported in the following platforms:

- Mobility RFS4000 Controller
- Mobility RFS6000 Controller
- Mobility RFS7000 Controller

Syntax

```
{no} country-code <code>
```

Parameters

<code>	A two (2) letter ISO-3166 country code. To view country codes, use the `show wireless country-code-list` command.

Usage Guidelines

`{no} country-code` erases all existing radio configuration.

Example

```
RFController(config)#country-code ?
  WORD  the 2 letter ISO-3166 country code ("show wireless country-code-list"
to see list of supported countries)

RFController(config)#no country-code US
RFController(config)#
```

crypto

Global Configuration commands

Use crypto to define system level local ID for ISAKMP negotiation and to enter the ISAKMP Policy, ISAKMP Client or ISAKMP Peer command set.

NOTE

`crypto isakmp(policy)Priority` moves to the `config-crypto-isakmp` instance. For more information, see *Crypto-isakmp Instance on page 327*.

`crypto isakmp client configuration group default` moves you to the `config-crypto-group` instance. For more details, see *Crypto-group Instance on page 341*.

`crypto isakmp peer IP Address` moves to the `config-crypto-peer` instance. For more details, see *Crypto-peer Instance on page 351*.

`crypto ipsec transformset <tag> <value>` leads you to `crypto-ipsec`. Use the crypto ipsec transform-set command to define the transform configuration for securing data (for example, esp-3des, esp-sha-hmac, etc.). The transform-set is assigned to a crypto map using the map's set transform-set command. For more details, see *Crypto-trustpoint Instance on page 387*.

`crypto pki trustpoint` mode leads to the `config-trustpoint` instance. For more details, see *Crypto-trustpoint Instance on page 387*.

Supported in the following platforms:

- Mobility RFS4000 Controller
- Mobility RFS6000 Controller
- Mobility RFS7000 Controller

Syntax

```
crypto [ipsec|isakmp|key|map|pki]

crypto ipsec [security-association|transform-set]
crypto ipsec security-association lifetime
       [kilobyte|seconds] <lifetime>
crypto ipsec transform-set <transform-set-tag>
       [ah-md5-hmac|ah-sha-hmac|esp-3des|esp-aes|esp-aes-192|
       esp-aes-256|esp-des|esp-md5-hmac|esp-sha-hmac]

crypto isakmp [client|keepalive|key|peer|policy]
crypto isakmp client configuration group default
crypto isakmp keepalive <10-3600>
crypto isakmp key [0 <secret>|2 <secret>|<secret>]
       [address <IP>|hostname <HOST>]
crypto isakmp peer [address <IP>|dn <distinguished-name>|
       hostname <HOST>]
crypto isakmp policy <1-10000>

crypto key [export|generate|import|zeroize]
crypto key export rsa <rsa-keypair> <URL> {<pass-phrase>}
```

```
crypto key generate rsa <rsa-keypair-name> <1024-2048>
crypto key import rsa <rsa-keypair-name> <URL>
       {<pass-phrase>}
crypto key zeroize rsa <rsa-keypair-name>

crypto map <crypto-map-tag> <1-1000> [ipsec-isakmp|ipsec-manual] {dynamic}

crypt pki [authenticate|enroll|export|import|trustpoint]
crypto pki authenticate <trust-point-name> [terminal|<URL>]
crypto pki enroll <trust-point-name> [request|self-signed]
crypto pki export <trust-point-name> [request|trustpoint]
       <URL>
crypto pki import <trust-point-name> [certificate|crl|
trustpoint]
crypto pki import <trust-point-name> certificate
       [<URL>|terminal]
crypto pki import <trust-point-name> crl <URL> <

crypto pki(authenticate|enroll|export|import|trustpoint)
crypto pki authenticate <name> (terminal|URL)
crypto pki enroll<name> (request|self-signed)
crypto pki [import|export] <name> (request|trustpoint)(URL)
crypto pki import ads [certificate|crl|trustpoint] (URL)(terminal)
```

Parameters

ipsec (security-association| transform-set)	Configures IPSEC policies.
	• security-association – Defines the security association parameter used to define its lifetime
	  • lifetime (kilobyte | seconds) – The lifetime of IPSEC security association. It can be defined in either:
	  kilobytes – Volume-based key duration, the minimum is 500 KB and maximum is 2147483646 KB .
	  seconds – Time-based key duration, the minimum is 90 seconds and maximum is 2147483646 seconds
	• transform-set [set name] – Uses the crypto ipsec transform-set command to define the transform configuration (authentication and encryption) for securing data
	  • ah-md5-hmac
	  • ah-sha-hmac
	  • esp-3des
	  • esp-aes
	  • esp-aes-192
	  • esp-aes-256
	  • esp-des
	  • esp-md5-hmac
	  • esp-sha-hmac
	The transform-set is then assigned to a crypto map using the map's set transform-set command. For more information, see *Crypto-map Instance on page 371*

isakmp [client|keepalive|key| peer|policy]	Configures the *Internet Security Association and Key Management Protocol* (ISAKMP) policy.
	• client configuration (group) (default) – Leads to the config-cryptogroup instance.
	For more details see *Crypto-group Instance on page 341*
	• keepalive <10-3600> – Sets a keepalive interval for use with remote peers. It defines the number of seconds between DPD messages
	• key [0 <key>|2 <key>|<key>] [address|hostname] – Sets a pre-shared key for remote peer
	  • 0 <key> – Password is specified unencrypted
	  • 2 <key> – Password is encrypted with password-encryption secret
	  • <key> – User provided password
	  • address – Defines a shared key with an IP address
	  • hostname – Defines the shared key with a hostname
	• peer [address|dn|hostname] – Sets the remote peer
	  • address – The IP address is the identity of the remote peer
	  • dn – The identity of the remote peer is the distinguished name
	  • hostname –The hostname is the identity of the remote peer
	• policy <1-10000> – Sets a policy for a ISAKMP protection suite

key [export|generate|import|zeroize]	Authentication key management functions.
	• export rsa <name> URL [tftp|ftp] – Exports a keypair related configuration
	• generate rsa <name> <1024-2048> – Generates a keypair
	  • <1024-2048> – Size of keypair in bits
	• import rsa <name> URL [tftp|ftp] – Imports keypair related configuration
	• zeroize rsa <name> – Deletes a keypair
	• rsa <identifier> – RSA keypair identifier associated with keypair
	• URL for sending the key, it can be one of the following:
	  • tftp://<IP>/path/file (or)
	  • ftp://<user>:<passwd>@<IP>/path/file

map <name> <sequence> [ipsec-isakmp| ipsec-manual] dynamic	Enter a crypto map. For more information, see *Crypto-map Instance on page 371*.
	• name <name> – Names the crypto map entry (not to exceed 32 characters)
	• <1-1000> – Sequence to insert into crypto map entry
	  • ipsec-isakmp – IPSEC w/ISAKMP
	  • ipsec-manual – IPSEC w/manual keying
	  • dynamic – Dynamic map entry (remote VPN configuration) for XAUTH with mode-config or ipsec-l2tp configuration

pki [authenticate|enroll| export|import|trustpoint]	Configures certificate parameters. The public key infrastructure is a protocol that creates encrypted public keys using digital certificates from certificate authorities. The PKI ensures each online party is who they claim to be.
	• authenticate <name> (terminal|tftp|ftp) – Defines the authenticate and import CA certificate
	• enroll <name> (request|self-signed) – Generates a certificate request or selfsigned certificate for the trustpoint
	• export <name> (request|trustpoint) (tftp|ftp) – Exports the trustpoint related configuration
	• import – Imports a trustpoint related configuration
	  • certificate – Imports server certificate for the trust point
	  • crl – certificate Revocation list
	  • URL – URL to get certificate from URLS:
	  tftp://<IP>/path/file
	  ftp://<user>:<passwd>@<IP>/path/file
	  • terminal – Copy and paste mode of enrollment
	  • trustpoint – Import trust point including either private key and server certificate or ca certificate or both
	• trustpoint – Creates and configures a trustpoint

Usage Guidelines

Follow the table to calculate how many character are required to add the key size for authentication and encryption. This is used while configuring Manual IPSEC only.

		AH-MD5	AH-SHA							
AH		32	40							
		ESP-MD5			ESP-SHA					
ESP-AUTH		Cipher	Auth		Cipher	Auth				
		16	16		20	20				
	DES		3DES		AES		AES-192		AES-256	
ESP-ENCR	Cipher	Auth	Cipher	Auth	Cipher	Auth	Cipher	Auth	Cipher	auth
	8	8	24	24	16	16	16	16	16	16

For example, To create a key with authentication type as ESP-SHA and encryption type as AES-192, enter 20+16=36 characters.

The key size for all the 3 different AES combinations is 128 bits or 16 bytes.

Follow the example below to see how the Auth and Encryption key is created in `(config)# crypto-ipsec` instance and used in `(config)# crypt-map` instance.

```
RFController(config)#crypto ipsec transform-set Test1 ?
  ah-md5-hmac   AH-HMAC-MD5 transform
  ah-sha-hmac   AH-HMAC-SHA transform
  esp-3des      ESP transform using 3DES cipher (168 bits)
  esp-aes       ESP transform using AES cipher
  esp-aes-192   ESP transform using AES cipher (192 bits)
  esp-aes-256   ESP transform using AES cipher (256 bits)
  esp-des       ESP transform using DES cipher (56 bits)
  esp-md5-hmac  ESP transform using HMAC-MD5 auth
  esp-sha-hmac  ESP transform using HMAC-SHA auth

RFController(config)#crypto ipsec transform-set Test1 esp-aes-192 esp-sha-hmac

RFController(config-crypto-ipsec)#exit

RFController(config)#crypto map TestMap-TechPub 10 ipsec-manual
RFController(config-crypto-map)#set peer 1.1.1.1
RFController(config-crypto-map)#match  address 101

RFController(config-crypto-map)#set transform-set tfset-manual

RFController(config-crypto-map)#set session-key inbound esp 257
cipher 12345678901234567890123456789012345678901234
authenticator 12345678901234567890123456789012345678901234


RFController(config-crypto-map)#set session-key outbound esp 258
cipher 12345678901234567890123456789012345678901234
authenticator 12345678901234567890123456789012345678901234

RFController(config-crypto-map)#exit

RFController(config)#interface vlan11

RFController(config-if)#crypto map manual
```

```
RFController(config-if)#show running-config
!
! configuration of Mobility RFS6000 Controller version 4.3.0.0
!
!
aaa authentication login default none
service prompt crash-info
!
username "admin" password 1 8e67bb26b358e2ed20fe552ed6fb832f397a507d

username "admin" privilege  superuser
username "operator" password 1 fe96dd39756ac41b74283a9292652d366d73931f
!
!
access-list 30 deny 11.1.1.0/24 log rule-precedence 10
access-list 101 permit ip 12.1.1.0/24 10.1.1.0/24 rule-precedence 10
access-list 102 permit ip 22.1.1.0/24 20.1.1.0/24 rule-precedence 10
mac access-list extended 200
permit any any type arp rule-precedence 10
!
.....................................................................
.....................................................................
.....................................
crypto isakmp key 0 12345678 address 11.1.1.1
crypto isakmp key 0 12345678 address 21.1.1.1
.....................................................
.....................................................
crypto ipsec transform-set tfset1 esp-3des esp-sha-hmac
mode tunnel
crypto ipsec transform-set tfset-manual esp-3des esp-sha-hmac
mode tunnel
!
crypto map MAP1 10 ipsec-isakmp
set peer 11.1.1.1
match address 101

set transform-set tfset1
set security-association level perhost
set security-association lifetime seconds 120
set security-association lifetime kilobytes 4608000
crypto map MAP2 10 ipsec-isakmp

set peer 21.1.1.1
match address 102


set transform-set tfset1
set security-association level perhost
set security-association lifetime seconds 120
set security-association lifetime kilobytes 4608000
crypto map remote 10 ipsec-isakmp dynamic

set peer 0.0.0.0
set remote-type xauth
crypto map manual 10 ipsec-manual
set peer 1.1.1.1
set session-key in esp 257 cipher 123456789012345678901234567890123456789012345678901234
authenticator 12345678901234567890123456789012345678901234
```

```
set session-key out esp 258 cipher
12345678901234567890123456789012345678901234 authenticator
12345678901234567890123456789012345678901234

match address 101

set transform-set tfset-manual
!
.....................................................
.....................................................
interface vlan11
ip address 11.1.1.2/24
crypto map manual
!
.....................................................
.....................................................
RFController(config-if)#
```

Usage Guidelines

A peer address can be deleted with a wrong isakmp value. Crypto currently matches only the IP address when a **no** command is issued

```
RFController(config)#crypto isakmp key 12345678 address 4.4.4.4

RFController(config)#show running-config
configuration of RFController version 4.2.1.0
version 1.0
!
service prompt crash-info
!
username admin password 1 8e67bb26b358e2ed20fe552ed6fb832f397a507d
username admin privilege  superuser
username operator password 1 fe96dd39756ac41b74283a9292652d366d73931f
username manager password 1 45b27d6483fc630981ad5096ff26a7956ce0c038
.....................................
.............................
crypto isakmp key 12345678 address 4.4.4.4
crypto ipsec security-association lifetime kilobytes 4608000
RFController(config)#

RFController(config)#no crypto isakmp key 12348 address 4.4.4.4
RFController(config)#
```

In the example above, **key 12345678** is associated with IP **address 4.4.4.4**. You can delete this key by using the no command and a wrong key number

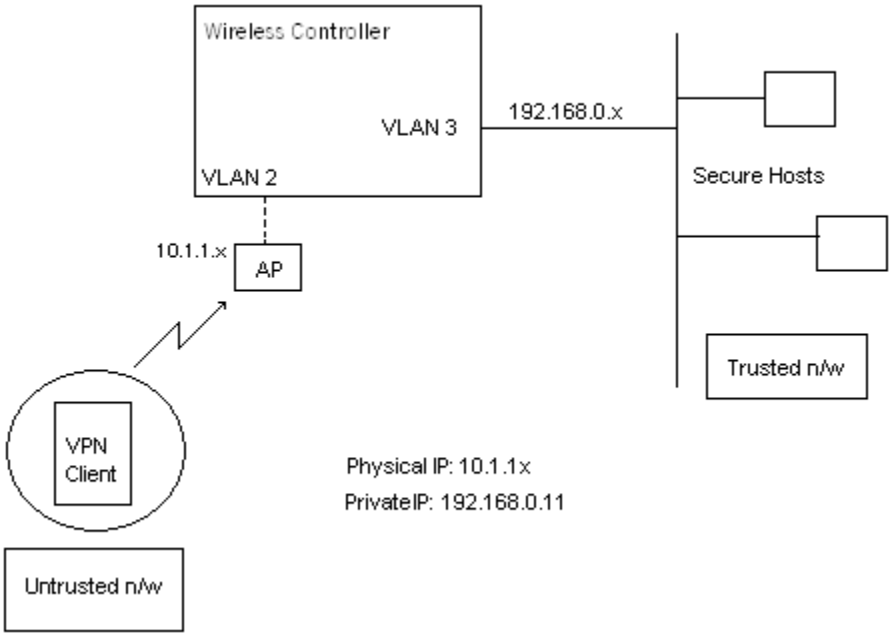
Example

```
RFController(config)#crypto pki ?
  authenticate  Authenticate and import CA Certificate
  enroll        Enroll
  export        Export
  import        Import
  trustpoint    Define a CA trustpoint

RFController(config)#crypto pki trustpoint ?
  WORD  Trustpoint Name

RFController(config)#crypto pki trustpoint Test
```

```
RFController(config-trustpoint)#?
Trustpoint Config commands:
  clrscr        Clears the display screen
  company-name  Company Name(Applicable only for request)
  email         email
  end           End current mode and change to EXEC mode
  exit          End current mode and down to previous mode
  fqdn          Domain Name Configuration
  help          Description of the interactive help system
  ip-address    Internet Protocol (IP)
  no            Negate a command or set its defaults
  password      Challenge Password(Applicable only for request)
  rsakeypair    Rsa Keypair to associate with the trustpoint
  service       Service Commands
  show          Show running system information
  subject-name  Subject Name is a collection of required parameters
                to configure a trustpoint.

RFController(config-trustpoint)#
```

Use Case 1: Configuring Remote VPN

Let us review an example of a wireless client connected to the controller. Assume it wants access to the corporate (trusted network) using IPSec VPN functionality.



A Brocade client is associated to a WLAN (say wlan1) attached to vlan2 on the controller. vlan2 is on subnet 10.1.1.x and is running a DHCP server that assigns IP addresses for this subnet. The corporate is on vlan3 of the controller, which has 192.168.0.x subnet.

The client being associated to wlan1 has an IP address of 10.1.1101x and wants to access the 192.168.0.x network securely.

In case the client is VPN enabled, it initiates a connection with the VPN server on our controller, the “conversation” that occurs between the peers consists of device authentication via Internet Key Exchange (IKE), followed by user authentication using IKE *Extended Authentication* (Xauth), push client relate configuration (using Mode Configuration), and IPsec security association (SA) creation.

Depending on the controller IPSec configuration (as discussed in the previous sections), the client establishes an IKE SA, and if the controller is configured for Xauth, the client waits for a "username/password" challenge and then responds to the challenge of the controller.

If the controller indicates that authentication is successful, the client requests further configuration parameters from the controller. At this stage, the private IP address (mode-config) is pushed to the client from a private address pool, configured for remote VPN clients. IPsec SA’s are created and the connection is complete.

Once the client has got a virtual IP, further packets from the client within the IPSec tunnel are routed to the corresponding VLAN interface (in our case vlan3), and the client gets access to the network. The IPSec tunnel is only between the client and the controller. After that the packets on the trusted side are sent without encryption.

NOTE
The example below is for a IPSec-L2TP connection over a wireless client. Use a windows default client for this configuration.

1. Create and configure a WLAN.

```
RFController(config)#
RFController(config)#wireless
RFController(config-wireless)#wlan 2 enable
RFController(config-wireless)#wlan 2 ssid MONARCH2
RFController(config-wireless)#wlan 2 vlan 2
```

2. Create and configure DHCP.

```
RFController(config)#ip dhcp pool vlan2
RFController(config-dhcp)#address range 10.1.1.2 10.1.1.254
RFController(config-dhcp)#default-router 10.1.1.1
RFController(config-dhcp)#network 10.1.1.0/24
```

3. Create and configure a VLAN interface named vlan2.

```
RFController(config)#interface vlan2
RFController(config-if)#ip address 10.1.1.1/24
```

4. Create and configure another VLAN interface named vlan3.

```
RFController(config)#interface vlan 3
RFController(config-if)#ip address dhcp
```

Use the commands below to configure IPSec VPN on the controller:

1. Create an Extended ACL.

```
RFController(config-ext-nacl)#ip access-list extended 101
```

2. Configure the local subnet and remote subnet as interesting traffic.

```
RFController(config-ext-nacl)# permit ip 10.1.1.0/24 any
RFController(config-ext-nacl)# permit ip 192.168.0.0/24 any
```

3. Configure a private pool address.

```
RFController(config)# ip local pool lo 192.168.0.2 hi 192.168.0.10
```

4. Specify DNS/WINS for the remote client.

```
RFController(config)#crypto isakmp client configuration group default
RFController(config-crypto-group)#dns 10.1.1.1
RFController(config-crypto-group)#wins 10.1.1.1
```

5. Specify the authentication type.

```
RFController(config)# aaa vpn-authentication local
RFController(config)# local username harry password brocade123
```

6. Create a transform set.

```
RFController(config)#crypto ipsec transform-set windows esp-3des esp-sha-hmac
RFController(config-crypto-ipsec)#mode transport
```

7. Specify a dynamic crypto map.

```
RFController(config)#crypto map TestMap 30 ipsec-isakmp dynamic
RFController(config-crypto-map)#set peer 0.0.0.0
RFController(config-crypto-map)#match address 101
RFController(config-crypto-map)#set transformset windows
RFController(config-crypto-map)#set remote-type ipsec-l2tp
```

8. Apply the crypto map to interface vlan2.

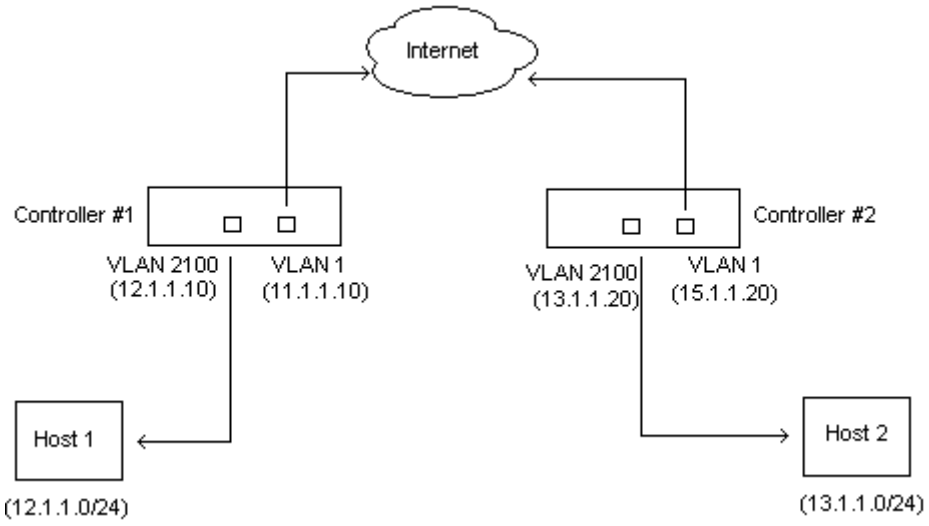
```
RFController(config)#interface vlan2
RFController(config-if)cryto map TestMap
```

9. Upon a successful connection, the XP client will obtain a virtual IP address.

Use Case 2: Configuring Site-to-Site VPN

Intranets use unregistered addresses connected over the public internet by site-to-site VPN. In this scenario, NAT is required for the connections to the public internet. However NAT is not required for traffic between the two intranets, which can be transmitted using a VPN tunnel over the public Internet.

The site-to-site VPN allows branch office mobility controllers to connect back to the central office using a secure, encrypted tunnel, for all site-to-site traffic. This allows a wired LAN in the branch office to bridge directly to the central site while maintaining full security.



This example requires two controllers. It can be configured with the following commands:

1. Configuration required on controller 1:

   a. Create an extended ACL. This is used to define the tunnel used by the traffic.

```
RFController(config)#access-list 150 permit ip 12.1.1.0/24 13.1.1.0/24
rule-precedence
```

   b. Create and configure ISAKMP parameters.

```
RFController(config)#crypto isakmp keepalive 10
RFController(config)#crypto isakmp key ADBROCADE address 15.1.1.20
RFController(config)#crypto ipsec security-association lifetime
kilobytes 4608000
```

   c. Create and configure ISAKMP policy.

```
RFController(config)#crypto isakmp policy 199
RFController(config-crypto-isakmp)#encryption aes
RFController(config-crypto-isakmp)#hash sha
RFController(config-crypto-isakmp)#authentication pre-share
RFController(config-crypto-isakmp)#group 5
RFController(config-crypto-isakmp)#lifetime 9496
```

   d. Create and configure an IPSec transform set.

```
RFController(config)#crypto ipsec transform-set TFSET ah-sha-hmac esp-aes
RFController(config-crypto-ipsec)#mode tunnel
```

   e. Create and configure a crypto map.

```
RFController(config)#crypto map THIRDMAP 435 isakmp
RFController(config-crypto-map)#set peer 15.1.1.20
RFController(config-crypto-map)#match address 150
RFController(config-crypto-map)#set transformset TFSET
RFController(config-crypto-map)#set security-association lifetime seconds 3600
```

   f. Associate the crypto map with a VLAN interface.

```
RFController(config)#interface vlan1
RFController(config-if)#ip address 11.1.1.10/24
RFController(config-if)#crypto map THIRDMAP
RFController(config-if)#interface vlan2100
RFController(config-if)#ip address 12.1.1.10/24
RFController(config-if)#ip route 0.0.0.0/0 11.1.1.2
```

2. Configuration required on controller 2:

   a. Create an extended ACL. This defines the tunnel used by the traffic.

```
RFController(config)#access-list 155permit ip 13.1.1.0/24 12.1.1.0/24
rule-precedence 1
```

   b. Create and configure the ISAKMP parameters.

```
RFController(config)#crypto isakmp keepalive 10
RFController(config)#crypto isakmp key ADBROCADE address 11.1.1.10
RFController(config)#crypto ipsec security-association lifetime
kilobytes 4608000
```

   c. Create and configure ISAKMP policy.

```
RFController(config)#crypto isakmp policy 100
RFController(config-crypto-isakmp)#encryption aes
RFController(config-crypto-isakmp)#hash sha
RFController(config-crypto-isakmp)#authentication pre-share
RFController(config-crypto-isakmp)#group 5
RFController(config-crypto-isakmp)#lifetime 9496
```

d. Create and configure IPSec an transform set.

```
RFController(config)#crypto ipsec transform-set TFSET ah-sha-hmac esp-aes
esp-sha-hmac
RFController(config-crypto-ipsec)#mode tunnel
```

e. Create and configure a crypto map.

```
RFController(config)#crypto map THIRDMAP 435 isakmp
RFController(config-crypto-map)#set peer 11.1.1.10
RFController(config-crypto-map)#match address 150
RFController(config-crypto-map)#set transformset TFSET
RFController(config-crypto-map)#set security-association lifetime seconds 3600
```

f. Associate the crypto map with a VLAN interface.

```
RFController(config)#interface vlan1
RFController(config-if)#ip address 15.1.1.20/24
RFController(config-if)#crypto map THIRDMAP
RFController(config-if)#interface vlan2100
RFController(config-if)#ip address 13.1.1.20/24
RFController(config-if)#ip route 0.0.0.0/0 15.1.1.2
```

do

Global Configuration commands

Runs commands from either the User Exec or Priv Exec mode

Supported in the following platforms:

- Mobility RFS4000 Controller
- Mobility RFS6000 Controller
- Mobility RFS7000 Controller

Syntax

```
do <privilege mode commands>
```

Parameters

None

Example

```
RFController(config)#do ping 157.235.208.69
PING 157.235.208.69 (157.235.208.69): 100 data bytes
128 bytes from 157.235.208.69: icmp_seq=0 ttl=64 time=0.1 ms
128 bytes from 157.235.208.69: icmp_seq=1 ttl=64 time=0.0 ms
128 bytes from 157.235.208.69: icmp_seq=2 ttl=64 time=0.0 ms
128 bytes from 157.235.208.69: icmp_seq=3 ttl=64 time=0.0 ms
128 bytes from 157.235.208.69: icmp_seq=4 ttl=64 time=0.0 ms

--- 157.235.208.69 ping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max = 0.0/0.0/0.1 ms
RFController(config)#
```

NOTE
In the example above, `ping` is a PRIV EXEC command.

end

Global Configuration commands

Ends the current mode and changes to the EXEC mode

Supported in the following platforms:

- Mobility RFS4000 Controller
- Mobility RFS6000 Controller
- Mobility RFS7000 Controller

Syntax

```
end
```

Parameters

None.

Example

```
RFController(config)#end

RFController#?
Priv Exec commands:
  acknowledge    Acknowledge alarms
  archive        Manage archive files
  autoinstall    autoinstall configuration command
  cd             Change current directory
  ........................................
  ........................................
```

errdisable

Global Configuration commands

Enables the timeout mechanism for the port to be enabled back after an error

Supported in the following platforms:

- Mobility RFS4000 Controller
- Mobility RFS6000 Controller
- Mobility RFS7000 Controller

Syntax

```
errdisable recovery [cause bpduguard|interval <10-1000000>]
```

Parameters

recovery [cause bpduguard| interval <10-1000000>]	Enables the timeout mechanism for the port to recover after an error. • cause bpduguard – Recover from an error condition caused due to bpduguard • interval <10-1000000> – The time interval after which a port is recovered or enabled after an error condition

Usage Guidelines

Use `no` command with `errdisable` parameter to the disable bridge timeout mechanism for the port

Example

```
RFController(config)#errdisable recovery interval 100
RFController(config)#

RFController(config)#errdisable recovery cause bpduguard
RFController(config)#

RFController(config)#no errdisable recovery cause bpduguard
RFController(config)#
```

ftp

Global Configuration commands

Configures the controller as an FTP server

Supported in the following platforms:

- Mobility RFS4000 Controller
- Mobility RFS6000 Controller
- Mobility RFS7000 Controller

Syntax

```
ftp [enable|password|rootdir|username]
ftp password [0 <secret>|1 <secret>|<secret>]
ftp rootdir <DIR>
ftp username <LINE>
```

Parameters

enable	Enables the FTP server
password [0 <secret>| 1 <secret>|<secret>]	Configures the FTP password. Set the password using one of the following options: • 0 <secret> — Password <secret> is specified unencrypted • 1 <secret> — Password <secret> is encrypted with SHA1 algorithm • <secret> — The password
rootdir <DIR>	Configures the FTP root dir. Set the ROOT directory location of the FTP server using: • <DIR> — The root directory for the ftp server
username <LINE>	Configures the FTP username. • <LINE> — The username for the ftp server.

Usage Guidelines

NOTE
The string size of encrypted password (option 1, Password is encrypted with SHA1 algorithm) must be exactly 40 characters.

Example

```
RFController(config)#ftp enable
RFController(config)#
```

hostname

Global Configuration commands

Changes the system's network name

Supported in the following platforms:

- Mobility RFS4000 Controller
- Mobility RFS6000 Controller
- Mobility RFS7000 Controller

Syntax

```
hostname <host-name>
```

Parameters

<host-name>	The name of the controller. This name is displayed when the controller is accessed from any network

Example

```
RFController(config)#hostname myRFController
myRFController(config)#
```

interface

Global Configuration commands

Configures a selected interface

This command is used to enter the interface configuration mode for the specified physical *Controller Virtual Interface* (SVI) interface. If the VLANx (SVI) interface does not exist, it is automatically created.

Supported in the following platforms:

- Mobility RFS4000 Controller
- Mobility RFS6000 Controller
- Mobility RFS7000 Controller

NOTE
The interfaces mentioned below are supported in the following platforms:
- ge <index> – Mobility RFS7000 Controller supports 4 GEs, Mobility RFS6000 Controller supports 8 GEs and Mobility RFS4000 Controller supports 5 GEs
- sa <index> – Mobility RFS7000 Controller supports 4 SAs and Mobility RFS4000 Controller supports 6 SAs
- me1 – Supported with Mobility RFS7000 Controller, Mobility RFS4000 Controller and Mobility RFS6000 Controller
- up1 – Supported with Mobility RFS6000 Controller and Mobility RFS4000 Controller.

NOTE
The interface mode leads to the `config-if` instance. For more information, see *Interface Instance on page 403*. The prompt changes from `RFController(config) #` to `RFController(config-if)`

Syntax (Mobility RFS7000 Controller)

```
interface [<interface-name>|ge <1-4>|me1|sa <1-4>|vlan <1-4094>]
```

Syntax (Mobility RFS6000 Controller)

```
interface [<interface-name>|ge <1-8>|me1|up1|vlan <1-4094>]
```

Syntax(RFS4000)

```
interface [<interface-name>|ge <1-5>|me1|up1|sa <1-6>|vlan <1-4094>|wwan]
```

Parameters

<interface-name>	The name of the interface that is selected.
ge <1-8>	Gigabit Ethernet interface (4 for Mobility RFS7000 Controller and 8 for Mobility RFS6000 Controller)
me1	Fast Ethernet interface
sa <1-4>	Static Aggregate interface (in Mobility RFS7000 Controller only)
up1	WAN interface (in Mobility RFS6000 Controller only)
vlan <1-4094>	Defines the VLAN interface

Usage Guidelines

Use the `no interface <interface-name>` to delete the specified SVI. Valid interfaces include all VLAN interfaces.

Example

```
RFController(config)#interface ge 2
RFController(config-if)#
```

ip

Global Configuration commands

Configures a selected *Internet Protocol* (IP) component

Supported in the following platforms:

- Mobility RFS4000 Controller
- Mobility RFS6000 Controller
- Mobility RFS7000 Controller

NOTE
Using **`access-list extended`** moves you to the **`(config-ext-nacl)`** instance. For more information, see *Chapter 14, Extended ACL Instance*.

Using **`access-list standard`** moves you to the **`(config-std-nacl)`** instance. For more information, see *Chapter 15, Standard ACL Instance*.

Using **`ip dhcp pool <pool-name>`** command to move to the **`(config-dhcp)`** instance. For additional information, see *Chapter 17, DHCP Server Instance*.

Using **`ip dhcp class <class-name>`** moves you to the **`(config-dhcpclass)`** instance. For additional information, see *Chapter 18, DHCP Class Instance*.

Syntax

```
ip [access-list|default-gateway|dhcp|domain-lookup|
       domain-name|dos|http|http-https|igmp|local|name-server|nat|route|
       routing|ssh|telnet]
ip [domain-lookup|routing]

ip access-list [standard|extended]
ip access-list extended [<100-199|<2000-2699>|<acl-name>]
ip access-list standard [<1-99>|<1300-1999>|<acl-name>]

ip default-gateway <IP>

ip dhcp [bootp|class|excluded-address|option|ping|pool]
ip dhcp bootp ignore
ip dhcp class <class-name>
ip dhcp excluded-address <IP-range-low> {<IP-range-high>}
ip dhcp option <option-name> <option-code> [ascii|ip]
ip dhcp ping timeout <1-10>
ip dhcp pool <pool-name>

ip domain-name <domain-name>

ip dos [ascend|bcast-mcast-icmp|chargen|enable|fraggle|
       ftp-bounce|invalid-protocol|option-route|router-solicit|router-advt|
       smurf|snork|tcp-intercept|tcp-max-incomplete|twinge]
       log [<0-8>|alerts|critical|debugging|emergencies|error|
       informational|none|notifications|warnings]

ip http [secure-server|secure-trustpoint|server]
ip http [secure-server|server]
ip http secure-trustpoint <trustpoint-name>
```

```
ip http-https [inactivity-timeout <1-1440>|
max-simultaneous-sessions-per-user <1-100>]

ip igmp snooping {[querier|unknown-multicast-fwd|vlan]}
ip igmp snooping {querier {[address|max-response-time|
       query-interval|timer|version]}}
ip igmp snooping {querier {address <IP>}}
ip igmp snooping {querier {max-response-time <1-25>}}
ip igmp snooping {querier {query-interval <1-18000>}}
ip igmp snooping {querier {timer expiry <60-300>}}
ip igmp snooping {querier {version <1-3>}}
ip igmp snooping {unknown-multicast-fwd}
ip igmp snooping {vlan [<1-4094>|<vlan-list>]
       {mrouter|querier|unknown-multicast-fwd]}
ip igmp snooping {vlan [<1-4094>|<vlan-list>]
       mrouter [interface <interface-list>|learn pim-dvmrp]
ip igmp snooping {vlan [<1-4094>|<vlan-list>]
       querier {[address|max-response-time|query-interval|timer|
       version]}}
ip igmp snooping {vlan [<1-4094>|<vlan-list>]
       unknown-multicast-fwd}

ip local pool default low-ip-address <low-IP> {high-ip-address <high-IP>}

ip name-server <IP>

ip nat [inside|outside] [destination|source]
ip nat inside destination static <IP> <port>
       [tcp|udp] <outside-global-IP> {<outside-port>}
ip nat inside destination static <IP> {<outside-global-IP>
       <outside-port>}
ip nat inside source list <acl-name> interface [<interface-name>|vlan
<1-4094>] overload
ip nat inside source static <local-IP> <outside-global-IP>
ip nat outside destination static <IP> <outside-port>
       [tcp|udp] {<inside-global-IP> {<inside-port>}}
ip nat outside destination static <IP> {<outside-global-IP>
       <outside-port>}
ip nat outside source list <acl-name> interface [<interface-name>|vlan
<1-4094>] overload
ip nat inside source static <local-IP> <outside-global-IP>

ip route [<IP-destination-prefix>
<IP-destination-prefix-mask>|<IP-destination-prefix/Mask>] <gateway-IP>

ip ssh {[port <port>|rsa keypair-name <key-pair-name>]}

ip telnet {port <port>}
```

Parameters

ip access-list extended [<100-199|<2000-2699>|<acl-name>] ip access-list standard [<1-99>|<1300-1999>|<acl-name>]	Using the access list parameter options to enter the **ext-nacl** context and the **std-nacl** context. The prompt changes to the context entered. • For more information on extended ACL, see *Chapter 14, Extended ACL Instance* • For more information on standard ACL, see *Chapter 15, Standard ACL Instance*
default-gateway <IP>	Configures the IP address of the default gateway • <IP> – IP address of the next-hop router

ip dhcp [bootp|class|excluded-address|option|ping|pool]	DHCP server configuration.
	• bootp ignore – Defines the BOOTP specific configuration
	  • ignore – Configures the DHCP server to ignore BOOTP requests
	• class <class-name> – Defines a DHCP class and enters the DHCP class configuration mode
	  • <class-name> – The DHCP class name
	• excluded-address <IP-range-low> *{<IP-range-high>}* – Prevents the DHCP server from assigning certain addresses
	  • <ip-range-low> – For IP range, the lower IP number. Enter this value for a single IP address
	  • <ip-range-high> – Optional. For IP range, the higher IP number
	• option <option-name> <option-code> [ascii|ip] – Defines the DHCP server's option name
	  • <option-name> – Defines the name of the option
	  • <option-code> – Defines option code, a value in the range of 0 to 254
	  • ascii – Specify the option type as ascii
	  • ip – Specify the option type as ip
	• ping timeout <1-10> – Specifies DHCP server's ping timeout in seconds
	• pool <pool-name> – Configures the DHCP server's address pool <pool-name>. This opens the **(config-dhcp)** instance. For more information, see *Chapter 17, DHCP Server Instance*

domain-lookup	Enables the DNS based name to address translation on the controller.
domain-name <domain-name>	Sets the domain name for the controller. • <domain-name> – The domain name string
http [secure-server|secure-trustpoint|server]	*Hyper Text Transfer Protocol* (HTTP) configuration. • secure-server – Sets the device to start the *Secure HTTP Server* (HTTPS) • secure-trustpoint <trustpoint-name> – Sets the name of the trustpoint used for secure connection to <trustpoint-name> • server – Sets device to start the HTTP server

local pool default low-ip-address <low-IP> *{high-ip-address <high-IP>}*	Sets the VPN local IP pool configuration
	• pool default low-ip-address <low-IP> *{high-ip-address <high-IP>}* – Specifies the address range for the default group tag
	  • low-ip-address <low-IP> – Specifies the lowest range for IP address assignment
	  • high-ip-address <high-IP> – Optional. Specifies the highest range for IP address assignment

name-server <IP>	Specifies the DNS server for the DHCP client. A maximum of 6 name servers can be configured. Servers are tried in the order entered. • <IP>– IP address of DNS server

nat [inside|outside] [destination|source]	Defines *Network Address Translation* (NAT) configuration values. These following commands are possible for NAT
	• **ip nat [inside|outside] destination** static <IP> <port> [tcp|udp] <outside-global-IP> *{<outside-port>}* – Sets the parameters for translation for inside destination
	• **ip nat [inside|outside] destination** static <IP> <outside-global-IP> {<outside-port>}– Sets the parameters for translation for inside destination
	  • inside – Indicates inside address translation
	  • outside – Indicates outside address translation
	  • destination – Indicates destination address translation
	  • static – Specifies local -> global address mapping
	  • <IP> – The local IP address
	  • <port> – Specifies the outside local port number
	  • [tcp|udp] – Specifies the protocol
	  • <outside-global-IP> – Specifies the outside global IP address to translate to
	  • <outside-port> – Optional. Specifies the outside port. Value in the range 1 to 65535
	• **ip nat [inside|outside] source** list <acl-name> interface [<interface-name>|vlan <1-4094>] overload – Sets the parameters for translation for inside sources
	  • inside – Indicates inside address translation
	  • outside – Indicates outside address translation
	  • source – Indicates source address translation
	  • list <acl-name> – Specifies the ACL name <acl-name> that describes local addresses
	  • interface [<interface-name>|vlan <1-4094>] – The interface to apply address translation to. Specify an interface name <interface-name>, or use a VLAN ID <1-4094>
	  • overload – Over loads the NAT address translation

	• **ip nat [inside|outside] source** static <outside-global-IP> <local-IP> – Sets the parameters for translation for inside sources
	  • inside – Indicates inside address translation
	  • outside – Indicates outside address translation
	  • source – Indicates source address translation
	  • static – Specifies local -> global address mapping
	  • <outside-global-IP> – The static global IP address to map from
	  • <local-IP> – The local IP address to map to

route [<IP-destination-prefix> <IP-destination-prefix-mask>|<IP-destination-prefix/Mask>] <gateway-IP>	Adds a static route entry in the routing table. • <IP-destination-prefix>– IP destination prefix • <IP-destination-prefix-mask> – Mask for the <IP-destination-prefix> IP • <IP-destination-prefix/Mask> – IP destination prefix with mask • <gateway-IP> – IP address of the next hop used to reach the destination
routing	Turns on IP routing
ssh *{[port <port>|rsa keypair-name <key-pair-name>]}*	Sets up the Secured Shell (SSH) server • port <port> – Optional. Defines the listening port (set between 0-65536) • rsa keypair-name <key-pair-name> – Optional. Sets the RSA encryption key used for configuring RSA keypair
telnet *{port <port>}*	Configures the Telnet server. • port <port> – Optional. Defines the listening port ID (set between 0-65535)

dos [ascend|
bcast-mcast-icmp|
chargen|enable|fraggle|
ftp-bounce|
invalid-protocol|
option-route|router-advt|
router-solicit|smurf|
snork|tcp-intercept|
tcp-max-incomplete|
twinge]
log [<0-8>|
alerts|
critical|
debugging| |emergencies|
errors|
informational|
none|
notifications|
warnings]
	Configures the *Denial of Service* (DOS) attack parameters.
	• ascend – Enables Ascend DoS checks
	• bcast-mcast-icmp – Detects Broadcast/Multicast Icmp traffic as attack
	• chargen – Enables chargen DoS checks
	• enable – Enables all DoS checks
	• fraggle – Enables fraggle DoS checks
	• ftp-bounce – Enables FTP bounce logs and sets the logging levels
	• invalid-protocol – Enables Invalid Protocol DoS attack check and sets the logging levels for this attack
	• option-route – Enables IP option route check
	• router-advt – Enables ICMP router advertisement check
	• router-solicit – Enables ICMP router solicit check
	• smurf log – Enables smurf attack check
	• snork – Enables check for packets
	• tcp-intercept – Enables TCP intercept
	• twinge – Enables twinge check
	For all the above DoS attacks, the following log options can be set.
	  • <0-8> – Select one numerical log level. All messages with and below this severity are logged
	  • emergencies – System is unusable (level 0)
	  • alerts – Immediate action needed (level 1)
	  • critical – Critical conditions (level 2)
	  • errors – Error conditions (level 3)
	  • warnings – Warning conditions (level 4)
	  • notifications – Normal but significant conditions (level 5)
	  • informational – Informational messages (level 6)
	  • debugging – Debugging messages (level 7)
	  • none –Disable logging (level 8)

	• tcp -max-incomplete –Configures the maximum half-open TCP connections in the system
	  • high <1-1000> – Sets the upper threshold value between 1 and 1000
	  • low <1 - 1000> – Sets the lower threshold value between 1 and1000

igmp snooping *{[querier|unknown-multicast-fwd|vlan]}*	Configures IGMP Snooping parameters.
	• unknown-multicast-fwd – Optional. Forwards packets from unregistered multicast servers
	• querier *{[address|max-response-time|query-interval|timer|version]}*– Configures IGMP querier. All options are optional
	  • address <IP> – Sets GMP querier source IP address
	  • max-response-time <1-25> – Sets IGMP querier maximum response time in seconds
	  • query-interval <1-18000> – Sets IGMP querier query interval
	  • timer expiry <60-300> – Sets querier other querier time out in seconds to a value in the range 60 to 300
	  • version <1-3> – Sets IGMP version
	• vlan [<1-4094>|<vlan-list>] *{mrouter|querier|unknown-multicast-fwd]}* – Identifies the vlan to use. All options are optional
	  • vlan <1-4094>|<vlan-list>] – Sets the vlan to use for IGMP Snooping
	  • <1-4094> – A single VLAN ID
	  • <vlan-list> – A list of VLAN IDs
	  • mrouter [interface <interface> |learn pim-dvmrp] – Sets information for Multicast router
	  • interface <interface> – Gigabit Ethernet interfaces to be configured. <interface> can be a single interface or a list of interfaces
	  • learn pim-dvmrp – The multicast controller learning protocol using PIM-DVMRP protocol
	  • querier *{[address|max-response-time|query-interval|timer|version]}}* – Sets IGMP querier for the selected VLAN interface
	  • unknown-multicast-fwd – Forwards packets from unregistered multicast servers for this VLAN

Usage Guidelines

1. Use the `no` command along with ip to undo any IP based configuration.

```
[no] ip(access-list|default-gateway|dos|dhcp|domain-lookup|
domain-name|http|local|name-server|nat|route|routing|ssh|telnet)
```

2. When using the `ip access-list` parameter, enter the following contexts:
   - ext-nacl – Extended ACL. For more information, see *Chapter 14, Extended ACL Instance*
   - std-nacl – Standard ACL. For more information, see *Chapter 15, Standard ACL Instance*
   - dhcp – DHCP Server instance. For more information, see *Chapter 17, DHCP Server Instance*

- dhcpclass – DHCP User Class instance. For more information, see *Chapter 18, DHCP Class Instance*
- Clear the IP DHCP Binding using the *clear* command

NOTE
To delete Standard/Extended and MAC ACL use **no access-list <access-list name>** under the Global Config mode.

Usage Guidelines

To create a DHCP User Class:

Create a DHCP class

Create a USER class named **MC800**. The privilege mode changes to (config-dhcpclass).
RFController(config)#ip dhcp class RFControllerDHCPclass

```
RFController(config-dhcpclass)#
```

3. Create a Pool named **WID**, using `(config)#` mode

```
RFController(config)#ip dhcp pool WID
RFController(config-dhcp)#
```

4. Associate the DHCP class, created in Step 1 with the pool created in Step 3. The controller supports the association of only 8 CDHCP classes with a pool.

```
RFController(config-dhcp)#class RFControllerDHCPclass
RFController(config-dhcp-class)#
```

5. The controller leads you to a new mode (config-dhcp-class). Use this mode to add an address range used with the DHCP class associated with the pool.

```
RFController(config-dhcp-class)#address range 11.22.33.44
```

Example

```
RFController(config)#ip access-list extended TestACL
RFController(config-ext-nacl)#

RFController(config)#ip access-list standard TestStdACL
RFController(config-std-nacl)#

RFController(config)#ip dhcp pool TestPool
RFController(config-dhcp)#

RFController(config)#ip dhcp class TestDHCPclass
RFController(config-dhcpclass)#
```

license

Global Configuration commands

Adds a feature license

Supported in the following platforms:

- Mobility RFS4000 Controller
- Mobility RFS6000 Controller
- Mobility RFS7000 Controller

Syntax

```
license <feature> <license-key>
```

Parameters

<feature>	The feature for which the license is to be added
<license-key>	The license key for the feature.

Example

```
RFController(config)#show licenses
Serial Number 6283529900020
feature          license string   license value
usage
  AP                  48             4

RFController(config)#
RFController(config)#license AP <license string>
RFController(config)#
```

line

Global Configuration commands

Configures the terminal line

Opens the config-line mode, where you can configure the various parameters for the selected terminal.

Supported in the following platforms:

- Mobility RFS4000 Controller
- Mobility RFS6000 Controller
- Mobility RFS7000 Controller

Syntax

```
line [console|vty]
line console <0-0>
line vty <0-871> {<0-871>}
```

Parameters

line console <0-0>	Set the primary terminal line to 0
line vty <0-871> *{<0-871>}*	Sets the virtual terminal line to a value between 0 and 871. Optionally the last line number can also be set to a value between 0 and 871

Example

```
RFController(config)# line console 0
RFController(config)# line vty 0
RFController(config)# line vty 0 871
RFController(config)#
```

local

Global Configuration commands

Sets the username and password for local user authentication

Supported in the following platforms:

- Mobility RFS4000 Controller
- Mobility RFS6000 Controller
- Mobility RFS7000 Controller

Syntax

```
local username <username> password [<password>|0 <password>|
       2 <password>]
```

Parameters

username <username>	The username. A character string of up to 64 characters
password	The password for the selected username <username>. <password> is a character string of up to 21 characters. • 0 indicates that <password> is unencrypted • 2 indicates that <password> is encrypted with password-encryption secret

Example

```
RFController(config)#local username "Noble Man" password "Noble Soul"
```

logging

Global Configuration commands

Modifies message logging facilities

Supported in the following platforms:

- Mobility RFS4000 Controller
- Mobility RFS6000 Controller
- Mobility RFS7000 Controller

Syntax

```
logging [aggregation-time|buffered|cli-commands|console|facility|
       host|monitor|on|snmp-set|syslog]

logging aggregation-time <1-60>

logging [buffered|console|monitor|syslog] [<0-7>|alerts|
       critical|debugging|emergencies|errors|informational|
       notifications|warnings]

logging facility [local0|local1|local2|local3|local4|local5|
       local6|local7]

logging host <IP>
loggin on
```

Parameters

aggregation-time <1-60>	Sets the number of seconds for aggregating repeated messages. The value can be configured between 1-60 seconds.
buffered [<0-7>|alerts|critical|debugging|emergencies|errors|informational|notifications|warnings]	Sets the buffered logging level • <0-7> – Enter the logging severity level (0-7) • alerts – Immediate action needed, (severity=1) • critical – Critical conditions, (severity=2) • debugging – Debugging messages, (severity=7) • emergencies – System is unusable, (severity=0) • errors – Error conditions, (severity=3) • informational – Informational messages, (severity=6) • notifications – Normal but significant conditions, (severity=5) • warnings – Warning conditions, (severity=4)
console [<0-7>|alerts|critical|debugging|emergencies|errors|informational|notifications|warnings]	Sets the console logging level.
facility [local0|local1|local2|local3|local4|local5|local6|local7]	Syslog facility in which log messages are sent. • local0 – Syslog facility local0 • local1 – Syslog facility local1 • local2 – Syslog facility local2 • local3 – Syslog facility local3 • local4 – Syslog facility local4 • local5 – Syslog facility local5 • local6 – Syslog facility local6 • local7 – Syslog facility local7
host <IP>	Configures a remote host to receive log messages. • <IP>– Remote host's IP address.
monitor [<0-7>|alerts|critical|debugging|emergencies|errors|informational|notifications|warnings]	Sets the terminal lines logging level.
on	Enables the logging of system messages.
syslog [<0-7>|alerts|critical|debugging|emergencies|errors|informational|notifications|warnings]	Sets the syslog servers logging level.

Example

```
RFController(config)#logging on
RFController(config)#logging aggregation-time 20
RFController(config)#logging buffered critical
RFController(config)#logging console critical
RFController(config)#logging facility local6
RFController(config)#logging monitor emergencies
RFController(config)#logging syslog notifications
RFController(config)#show logging

Logging module: enabled
```

```
    Aggregation time: 30 seconds
    Console logging: level warnings
    Monitor logging: level emergencies
    Buffered logging: level warnings
    Syslog logging: level notifications
          Facility: local4

Log Buffer (75 bytes):

June 22 11:21:56 2010:  %PM-6-PROCSTART:  Starting Process "/usr/sbin/thttpd"

RFController(config)#
```

mac

Global Configuration commands

Configures MAC access lists (goes to the MAC ACL mode)

For more information on this mode, see *Chapter 16, Extended MAC ACL Instance*.

Supported in the following platforms:

- Mobility RFS4000 Controller
- Mobility RFS6000 Controller
- Mobility RFS7000 Controller

Syntax

```
mac access-list extended <mac-acl-name>
```

Parameters

access-list extended <mac-acl-name>	Defines the ACL configuration for the MAC address • extended <mac-acl-name>– MAC Extended ACL • <mac-acl-name> – Defines the name of the ACL

Usage Guidelines

To delete Standard/Extended and MAC ACL, use **`no access-list <access-list name>`** under the Global Config mode.

Example

```
RFController(config)#mac access-list extended Test1
RFController(config-ext-macl)#
```

NOTE
When using the **`ip access-list`** parameter, enter the following contexts: ext-macl — extended MAC ACL. For more details see *.Extended MAC ACL Instance on page 487*

mac-address-table

Global Configuration commands

Configures the MAC address table

Supported in the following platforms:

- Mobility RFS4000 Controller
- Mobility RFS6000 Controller
- Mobility RFS7000 Controller

Syntax

```
mac-address-table aging-time [0|<10-1000000>]
```

Parameters

aging-time [0|<10-1000000>]	The duration for which a learned mac address persists after the last update • 0 – Disables aging • <10-1000000> – Sets the aging time in seconds

Example

```
RFController(config)#mac-address-table aging-time 100
RFController(config)#
```

mac-name

Global Configuration commands

Sets a name to the MAC address

Supported in the following platforms:

- Mobility RFS4000 Controller
- Mobility RFS6000 Controller
- Mobility RFS7000 Controller

Syntax

```
mac-name <MAC> <mac-name>
```

Parameters

<MAC> <name>	The MAC address to set a ease-of-use name for.
<mac-name>	Sets the name <name> to the MAC address <MAC> for ease of use. <name> must be configured following the DNS naming convention.

Usage Guidelines

Use `(no) mac-name` to configure the clients name to its default. The default identity for an Client is its MAC address.

Example

```
RFController(config)#mac-name 06-bc-f3-00-a0-45 ServerTecDoc
RFController(config)#
RFController(config)#show mac-name
Index   MAC Address        MAC Name
  1     06-BC-F3-00-A0-45  ServerTecDoc
Number of MAC names configured = 1
RFController(config)#
```

management

Global Configuration commands

Sets management interface properties

Limits local access (through web/telnet) to management interfaces only.

Supported in the following platforms:

- Mobility RFS4000 Controller
- Mobility RFS6000 Controller
- Mobility RFS7000 Controller

Syntax

```
management secure
```

Parameters

secure	Limits local access (Web/Telnet etc.) to the management interface.

Example

```
RFController(config)#management secure
RFController(config)#
```

ntp

Global Configuration commands

Configure *Network Time Protocol* (NTP) values

Supported in the following platforms:

- Mobility RFS4000 Controller
- Mobility RFS6000 Controller
- Mobility RFS7000 Controller

Syntax

```
ntp [access-group|authenticate|authentication-key|autokey|
broadcast|broadcastdelay|master|peer|server|trusted-key]

ntp access-group [peer|query-only|serve|serve-only]
       [<1-99>|<100-199>|<1300-1999>|<2000-2699>]

ntp authenticate

ntp authentication-key <key> md5 [0 <secret>|2 <secret>|<secret>]

ntp autokey [client-only|host]

ntp broadcast [client|destination]
ntp broadcast destination <IP> {[key <1-65534>|version
       <1-4>]}

ntp broadcastdelay <1-999999>

ntp master {<1-15>}

ntp [server|peer] <peer-name-or-IP>
ntp [server|peer] <peer-name-or-IP>
       [autokey|key|prefer|version]
ntp [server|peer] <peer-name-or-IP> autokey
       {[prefer {verson <1-4>}|version <1-4> {prefer}]}
ntp [server|peer] <peer-name-or-IP> key <1-65534> [prefer
       {verson <1-4>}|version <1-4> {prefer}]
ntp [server|peer] <peer-name-or-IP> prefer {version <1-4>}
ntp [server|peer] <peer-name-or-IP> version <1-4> {prefer}

ntp trusted-key <1-65534>
```

Parameters

access-group [peer|query-only|serve| serve-only] [<1-99>| <100-199>|<1300-1999> | <2000-2699>]	Controls NTP access.
	• peer – Provides full access
	• query-only – Allows only control queries
	• serve – Provides server and query access
	• serve-only – Provides only server access
	  • <1-99> – Defines the standard IP access list
	  • <100-199> – Extended IP access list
	  • <1300-1999> – Standard IP access list (expanded range)
	  • <2000-2699> – Extended IP access list (expanded range)

authenticate	Authenticates time sources.

authentication-key <key> md5 [0 <secret>| 2 <secret>|<secret>]	Defines the authentication key for trusted time sources.
	• md5 – Sets MD5 authentication
	  • 0 <secret> – Password is specified unencrypted
	  • 2 <secret> – Password is specified encrypted with password-encryption secret
	  • <secret> – Authentication key

autokey [client-only|host]	Enables the NTP autokey authentication scheme. • client-only – The controller is a client to other trusted-hosts in the autokey group • host – Configures the controller as a trusted host

broadcast [client|destination]	Configures the NTP broadcast service.
	• client – Listens to NTP broadcasts
	• destination <IP> *{[key <1-65534>|version <1-4>]}*– Configures broadcast destination address
	  • IP Address – Defines the destination broadcast IP address
	  • key <1-65536> – Optional. Sets the broadcast key number
	  • version <1-4> – Sets the NTP version number
	NOTE: The controller acting as an NTP client will not associate to a broadcast IP (NTP Server) with no authentication i.e. without using symmetric key or auto-key

broadcastdelay <1-999999>	Defines the estimated round-trip delay. • <1-999999> – Sets the round-trip delay in microseconds
master *{<1-15>}*	Acts as a NTP master clock. • <1-15> – Optional. Sets the stratum number for the NTP master clock

peer <peer-name-or-IP> [autokey|key|prefer| version]	Configures the NTP peer.
	• <peer-name-or-IP> – Sets the IP address or name of the peer
	• autokey *{[prefer {version <1-4>}|version <1-4> {prefer}]}* – Configures an autokey peer authentication scheme
	  • prefer – Optional. Prefers this peer when possible
	  • version <1-4> – Optional. Configures the NTP version to use
	• key <1-65534> *{[prefer {version <1-4>}|version <1-4> {prefer}]}* – Configures the autokey peer authentication key
	  • key <1-65535> – Sets the peer authentication key number

	• prefer *{version <1-4>}* – Sets the preference for autokey. Optionally set the NTP version to use • version <1-4> *{prefer}* – Sets the NTP version to use. Optionally set this peer as preferred peer

server	Configures the NTP server.
	• <peer-name-or-IP> – Sets the IP address or name of the peer
	• autokey *{[prefer {version <1-4>}|version <1-4> {prefer}]}* – Configures an autokey peer authentication scheme
	  • prefer – Optional. Prefers this peer when possible
	  • version <1-4> – Configures the NTP version
	• key <1-65534> *{[prefer {version <1-4>}|version <1-4> {prefer}]}* – Configures the autokey peer authentication key
	  • key <1-65535> – Sets the peer authentication key number
	• prefer *{version <1-4>}* – Sets the preference for autokey. Optionally set the NTP version to use
	• version <1-4> *{prefer}* – Sets the NTP version. Optionally set this peer as preferred peer

trusted-key <1-65534>	Key numbers for trusted time sources. • <1-65534> – Defines the Key number

Example

```
RFController(config)#ntp peer ?
  WORD  Name/IP address of peer

RFController(config)#ntp peer TestPeer ?
  autokey  Configure autokey peer authentication scheme
  key      Configure peer authentication key
  prefer   Prefer this peer when possible
  version  Configure NTP version
  <cr>


RFController(config)#ntp peer TestPeer autokey ?
  prefer   Prefer this peer when possible
  version  Configure NTP version
  <cr>

RFController(config)#ntp peer TestPeer autokey prefer ?
  version  Configure NTP version
  <cr>

RFController(config)#ntp peer TestPeer autokey prefer version ?
  <1-4>  NTP version number

RFController(config)#ntp peer TestPeer autokey prefer version 3
RFController(config)#

RFController(config)#ntp peer TestPeer key ?
  <1-65534>  Peer key number

RFController(config)#ntp peer TestPeer key 20 ?
  prefer   Prefer this peer when possible
  version  Configure NTP version
  <cr>
```

```
RFController(config)#ntp peer TestPeer key 20 prefer ?
  version  Configure NTP version
  <cr>

RFController(config)#ntp peer TestPeer key 20 prefer version ?
  <1-4>  NTP version number

RFController(config)#ntp peer TestPeer key 20 prefer version 2
Invalid server name "TestPeer" provided. Please enter a valid name
RFController(config)#
```

prompt

Global Configuration commands

Configures and sets the systems prompt

Supported in the following platforms:

- Mobility RFS4000 Controller
- Mobility RFS6000 Controller
- Mobility RFS7000 Controller

Syntax

```
prompt <prompt>
```

Parameters

<prompt>	Enter the new prompt displayed by the system. The following operational modifiers are available.
	• %% – Displays the % sign
	• %h – Displays the host name
	• %m – Displays the current configuration mode
	• %n – Displays the CLI line
	• %p – Displays the privilege mode prompt sign
	  • > - User mode prompt
	  • # - Priv Exec mode prompt
	  • (config)# - Global Config mode prompt
	• %s – Displays a space
	• %t – Displays a tab space
	• %A – Displays date and time in ASCII format
	• %D – Displays date in MM/DD/YYYY format
	• %N – Displays a new line
	• %T – Displays time in the hh:mm:ss format

Example

```
RFController(config)#prompt NobleMan%s%h%m%p
NobleMan RFController(config)#
```

radius-server

Global Configuration commands

Enters the RADIUS server mode, the system prompt changes from the default config mode to the RADIUS server mode

Supported in the following platforms:

- Mobility RFS4000 Controller
- Mobility RFS6000 Controller
- Mobility RFS7000 Controller

NOTE
radius-server local mode takes you to the RADIUS server context. For more details see *Chapter 19, Radius Server Instance*.

Syntax

```
radius-server [host|key|local|retransmit|timeout]
radius-server host <IP>
radius-server key [0 <secret>|2 <secret>|<secret>]
radius-server local
radius-server retransmit <0-100>
radius-server timeout <1-1000>
```

Parameters

host <IP>	Specifies a RADIUS server. • <IP> – Defines the IP address of RADIUS server
key [0 <secret>| 2 <secret>|<secret>]	Sets the Encryption key shared with the RADIUS servers. • 0 <secret> – Password is specified unencrypted • 2 <secret> – Password is encrypted with password-encryption secret • <secret> – Text of shared key, up to 127 characters
local	Configures local RADIUS server parameters. This takes you to a new **config-radius-server** context. Refer to *Chapter 19, Radius Server Instance* for more details.
retransmit <1-100>	Specifies the number of retries to active server. • <0-100> – Number of retries for a transaction (default is 3)
timeout <1-1000>	Time to wait for a RADIUS server to reply. • <1-1000> – Wait time (default 5 seconds)

Usage Guidelines

The RADIUS server host is used to configure RADIUS server details. These details are required for management user authentication if AAA authentication has been defined as RADIUS

Example

```
RFController(config)#radius-server local
RFController(config-radsrv)#
```

ratelimit

Global Configuration commands

Configures rate limit parameters

Supported in the following platforms:

- Mobility RFS4000 Controller
- Mobility RFS6000 Controller
- Mobility RFS7000 Controller

Syntax

```
ratelimit [arp|bcast|mcast|ucast] [<0-7>|alerts|critical|
debugging|emergencies|errors|informational|notifications|
warnings]
```

Parameters

ratelimit [arp|bcast|mcast|ucast] [<0-7>|alerts|critical| debugging|emergencies| errors|informational| notifications|warnings]	Sets the logging levels for ratelimit feature.
	• [arp|bcast|mcast|ucast] – Sets the protocol
	  • <0-7> – Log severity level
	  • alerts – immediate action needed
	  • critical –Critical conditions
	  • debugging – Debugging messages
	  • emergencies – System is unusable
	  • errors – Error conditions
	  • informational – Informational messages
	  • notifications – Normal but significant conditions
	  • warnings – Warning conditions

Example

```
RFController(config)# ratelimit arp log 0
RFController(config)# ratelimit arp log emergencies
```

redundancy

Global Configuration commands

Configures redundancy group parameters

Supported in the following platforms:

- Mobility RFS4000 Controller
- Mobility RFS6000 Controller
- Mobility RFS7000 Controller

Syntax

```
redundancy [auto-revert|auto-revert-period|
       critical-resource-ip|dhcp-server|discovery-period|
       dynamic-ap-load-balance|enable|group-id|handle-stp|
       heartbeat-period|hold-period|interface-ip|manual-revert|
       member-ip|mode]

redundancy auto-revert enable
redundancy auto-revert-period <1-1800>
redundancy critical-resource-ip <IP>
redundancy dhcp-server enable
redundancy discovery-period <10-60>

redundancy dynamic-load-balance [enable|per-ap-client-threshold|
       schedule-interval|schedule-start-time|trigger]
redundancy dynamic-ap-load-balance enable
redundancy dynamic-ap-load-balance per-ap-client-threshold
       <1-512>
redundancy dynamic-ap-load-balance schedule-interval <1-336>
redundancy dynamic-ap-load-balance schedule-start-time
       <HH:MM> <1-31> <1-12> <2008-2035>
redundancy dynamic-ap-load-balance trigger
       [runtime|schedule]

redundancy enable
redundancy group-id <1-65535>
redundancy handle-stp enable
redundancy heartbeat-period <1-255>
redundancy hold-period <10-255>
redundancy interface-ip <IP>
redundancy manual-revert
redundancy member-ip <IP>
redundancy mode [primary|standby]
```

Parameters

auto-revert enable	Enables auto-revert.
auto-revert-period <1-1800>	Sets the redundancy auto-revert delay interval in minutes. The default is 5 minutes.
critical-resource-ip <ip_address>	Sets critical resource IP address. • <ip_address> – IP address of the critical resource
dhcp-server enable	Enables the DHCP redundancy protocol.
discovery-period <10-60>	Sets the redundancy discovery interval in seconds. The default is 30 seconds.
dynamic-ap-load-balance [enable| per-ap-client-threshold| schedule-interval| schedule-start-time| trigger]	Configures the different Dynamic AP Load Balance feature. The following are the configured options: • enable – Enables Dynamic AP Load Balance • per-ap-client-threshold <1-512> – Sets the threshold per-ap client value to trigger Dynamic AP Load Balance. Set a value between 1 & 512 • schedule-interval <1-336> – Sets the time interval days to trigger Dynamic AP Load Balance • schedule-start-time HH:MM <1-31> <1-12> <2008-2035> – Sets the scheduled start time for Dynamic AP Load Balance • trigger [runtime|schedule] – Sets the trigger for running Dynamic AP Load Balancing. Can be either runtime or schedule
enable	Enables the redundancy protocol.
group-id <1-65535>	Sets the cluster ID (default cluster ID is 1).
handle-stp enable	Delays the redundancy protocol state machine exec, considering STP.
heartbeat-period <1-255>	Sets the redundancy heartbeat interval.
hold-period <10-255>	Sets the redundancy hold interval.
interface-ip <IP>	Sets the redundancy interface IP address.
manual-revert	Reverts standby to non-active mode.
member-ip <IP>	Adds a member with the IP <IP> to this redundancy group.
mode [primary|standby]	Sets the mode to either primary or standby.

Example

```
RFController(config)#redundancy discovery-period 20
RFController(config)#

RFController(config)#redundancy handle-stp enable
RFController(config)#

RFController(config)#redundancy heartbeat-period 20
RFController(config)#

RFController(config)#redundancy hold-period 25
RFController(config)#

RFController(config)#redundancy mode primary
RFController(config)#
```

role

Global Configuration commands

Configures role parameters

NOTE
Opens the role configuration mode **(config-role)** to enable further configuration of the role. For Avance Security Licence must be installed for Role Based Firewall to work. Please contact customer support to purchase license for the same.

Supported in the following platforms:

- Mobility RFS4000 Controller
- Mobility RFS6000 Controller
- Mobility RFS7000 Controller

Syntax

```
role [<rolename>|assignment]

role <rolename> <priority>
role assignment immediate enable
```

Parameters

role <rolename> <priority>	Creates a new role with the name <rolename> and with the priority <priority> (range 1-10001). This moves to the role instance. For more information see *Chapter 26, Role Instance*.
role assignment immediate enable	Enables immediate role assignment and triggers role evaluation. This is required when a new role is added or a role is modified.

Usage Guidelines

To remove a role, use the command

```
{no} role <rolename> <priority>
```

Example

```
RFController(config)# role AccMgr 10
RFController(config-role)# ?

RFController(config)#role assignment immediate enable

RFController(config)#show role

role officeuser 10
 authentication-type any
 encryption-type any
 ap-location exact "office"
 essid office
 client-mac any
 group any

role globaluser 11
 authentication-type any
```

```
 encryption-type any
 ap-location any
 essid any
 client-mac any
 group any

role default-role 10001
 authentication-type any
 encryption-type any
 ap-location any
 essid any
 client-mac any
 group any
```

rtls

Global Configuration commands

Configures *Real Time Location System* (RTLS) parameters

This enables the Controller to provide complete visibility to the location of assets and thereby enabling location based service.

Supported in the following platforms:

- Mobility RFS4000 Controller
- Mobility RFS6000 Controller
- Mobility RFS7000 Controller

NOTE
`rtls` command instantiates **`(config-rtls)`** instance. For more details see *Chapter 21, RTLS Instance*. The prompt changes from `RFController (config)#` to `RFController (config-rtls)`

Syntax

```
rtls
```

Parameters

None

Example

```
RFController(config)#rtls
RFController(config-rtls)#
```

service

Global Configuration commands

Retrieves system data (tables, log files, configuration, status and operation) for debugging and problem resolution

Supported in the following platforms:

- Mobility RFS4000 Controller
- Mobility RFS6000 Controller
- Mobility RFS7000 Controller

To view the **service** command of User Exec and Priv Exec Mode, refer to *Chapter 2, service* command.

Syntax

```
service [advanced-vty|dhcp|diag|password-encryption|pm|
       prompt|radius|redundancy|set|show|stunnel|terminal-length|
       watchdog]
service [advanced-vty|dhcp|

service diag [enable|limit|period|tech-support-period|
       tech-spport-url]

service password-encryption <secret>
service pm sys-restart
service prompt crash-info
service radius {restart}
service redundancy dynamic-ap-load-balance start
service set [command-history|reboot-history|upgrade-history]
```

Parameters

advanced-vty	Enables advanced mode vty interface
dhcp	Enables the DHCP server service
diag [enable|limit|period|tech-support-period|tech-support-url]	Services diagnostics configuration. • enable – Enable in service diagnostics • limit – Displays diagnostic limit command • period <100-30000> – Sets diagnostics period • tech-support-period <10-10080> – Sets the tech support period. Default is 1440 minutes (1day) • tech-support-url <URL> – Sets the tech support URL to <URL>. This is used during auto generated tech support dumps

password-encryption secret 2 <secret>	Encrypts passwords in configuration.
	• secret 2 <secret> – Encrypt passwords with secret phrase
	  • 2 – Type of encryption SHA256-AES256
	  • <secret> – Passphrase for encryption

pm sys-restart	Process Monitor. • sys-restart – Enable PM to restart the system when a processes fails **Note:** The process restart is one count less than what is configured.
prompt crash-info	Enables crash-info prompt
radius *{restart}*	Enables RADIUS server. • restart – Restarts the RADIUS server
redundancy dynamic-ap-load-balance start	Starts Dynamic AP Load Balancing service for redundancy support.
set [command-history|reboot-history|upgrade-history]	Sets service parameters. • command-history <10-300> – Sets the number of previous commands to remember. Default 200 • reboot-history <10-100> – Sets the number of previous reboot details to remember. Default 50 • upgrade-history <10-100> – Sets the number of previous upgrade details to remember. Default 50
show cli	Shows running system information. Shows the CLI commands for the current mode.
terminal-length <0-512>	System wide terminal length configuration.
watchdog	Enables service for watchdog.

Usage Guidelines

The **`service password-encryption`** set by the user cannot be disabled without knowing the old password. Refer the note below for more clarification.

NOTE
The **no service password-encryption** command used to disable the encryption, now requires the user to know the old password. The user will have to enter the old password to disable the encryption.

Earlier, using **no service password-encryption** disabled the encryption and `show running config` displayed the passwords as plaintext.

Now, the user has to user **no service password-encryption <old password key>** to disable or change the password.

Example

```
RFController(config)#service dhcp
RFController(config)#

RFController(config)#service radius restart
RFController(config)#
```

smtp-notification

Global Configuration commands

Modifies SMTP notification parameters

Supported in the following platforms:

- Mobility RFS4000 Controller
- Mobility RFS6000 Controller
- Mobility RFS7000 Controller

Syntax

```
smtp-notification [authenticate|enable|password|port|prefix|
recipient|sender|smtp-server-address|user]

smtp-notification authentication enable

smtp-notification enable {traps [all|dhcp-server|
       diagnostics|miscellaneous|mobility|nsm|radius-server|
       redundancy|snmp|wireless]
smtp-notification enable traps all
smtp-notification enable traps dhcp-server
       {[dhcpServerDown|dhcpServerUp]}
smtp-notification enable traps diagnostics {[cpuLoad1Min|
       cpuLoad5Min|cpuLoad15Min|fanSpeedLow|fileDescriptors|
       ipRouteCache|packetBuffers|processMemoryUsage|ramFree|
       tempHigh|tempOver|usedKernelBuffer]}
smtp-notification enable traps miscellaneous
       {[caCertExpired|lowFsSpace|periodicHeartbeat|
       processMaxRestartsReached|savedConfigModified|
       serverCertExpired|controllerEvent]}
smtp-notification enable traps mobility {[operationallyDown|
       operationallyUp|peerDown|peerUp]}
smtp-notification enable traps nsm {dhcpIPChanged}
smtp-notification enable traps radius-server
       {[radiusServerDown|radiusServerUp]}
smtp-notification enable traps redundancy{[adoptionExceeded|
       criticalResourceDown|criticalResourceUp|
       grpAuthLevelChanged|memberDown|memberMisConfigured|
       memberUp]}
smtp-notification enable traps snmp {[authenticationFail|
       coldstart|linkdown|linkup]}
smtp-notification enable traps wireless {[ap-detection|ids|
       radio|self-healing|station|wlan]}
smtp-notification enable traps wireless ap-detection
       {[externalAPDetected|externalAPRemoved]}
smtp-notification enable traps wireless ids
       {[muExcessiveEvents|radioExcessiveEvents|
       controllerExcessiveEvents]}
smtp-notification enable traps wireless radio
{[adopted|unadopted|detectedRadar]}
smtp-notification enable traps wireless self-healing
       activated
smtp-notification enable traps wireless station
       {[associated|deniedAssociationAsPortCapacityReached|
       deniedAssociationOnCapability|deniedAssociationOnErr|
       deniedAssociationOnInvalidWPAWPA2IE|
```

```
        deniedAssociationOnRates|deniedAssociationOnShortPream|
        deniedAssociationOnSpectrum|deniedAssociationOnSSID|
        deniedAuthentication|disassociated|radiusAuthFailed|
        tkipCounterMeasures|vlanChanged]}
smtp-notification enable traps wireless wlan
        {[vlanUserLimitReached|webPortalUnavailable|
        webPortalUnreachable|webPortalUnconnected]}


smtp-notification password 0 <password>
smtp-notification port <1-65535>
smtp-notification prefix <smtp-prefix>
smtp-notification recipient <1-4> <recipient-address>
smtp-notification sender <sender-address>
smtp-notification smtp-server-address <IP>
smtp-notification user <username>
```

Usage Guidelines

It's recommended smtp-notification not be enabled for all traps. When smtp-notification is enabled, an email is sent to the recipients every time a trap is fired. An email is sent for each fired trap. This could potentially generate large email traffic for the recipients.

Some traps, such as Association, Disassociation, generate a large number of notifications which are then consolidated and sent as a single email every five (5) minutes.

When smtp-notification is enabled and the sender, recipient, server, and port values are not configured, then a syslog event "Incomplete Configuration" is fired every five (5) minutes till the issue is resolved.

Parameters

authenticate enable	Enables SMTP Server authentication.

enable traps [all|dhcp-server|diagnostics|miscellaneous|mobility|nsm|radius-server|redundancy|snmp|wireless]	Enables SMTP notification for traps.
	• all – Enables SMTP Notification for all traps
	• dhcp-server [dhcpServerDown|dhcpServerUp]– Enables dhcp-server traps
	  • dhcpServerDown – DHCP Server down
	  • dhcpServerUp – DHCP Server up
	• diagnostics [cpuLoad15Min|cpuLoad1Min|cpuLoad5Min|fanSpeedLow|fileDescriptors|ipRouteCache|packetBuffers|processMemoryUsage|ramFree|tempHigh|tempOver|usedKernelBuffer] – Enables diagnostics traps
	  • cpuLoad15Min – Average CPU load for last 15 minutes exceeds limit
	  • cpuLoad1Min – Average CPU load for last minute exceeds limit
	  • cpuLoad5Min – Average CPU load for last five minutes exceeds limit
	  • fanSpeedLow – Fan speed below limit
	  • fileDescriptors – File descriptor number exceeds limit
	  • ipRouteCache – IP route cache size exceeds limit
	  • packetBuffers – Packet buffer usage exceeds limit
	  • processMemoryUsage – Processor memory usage exceeds limit
	  • ramFree – RAM free space below limit
	  • tempHigh – Temperature exceeds high limit
	  • tempOver – Temperature exceeds critical limit
	  • usedKernelBuffer – Kernel buffer usage exceeds limit for some buffer size

	• miscellaneous [caCertExpired|lowFsSpace|periodicHeartbeat|processMaxRestartsReached|savedConfigModified|serverCertExpired|controllerEvent] – Enables miscellaneous traps
	  • caCertExpired – CA certificate has expired
	  • lowFsSpace – Available file system space is lower than the limit
	  • periodicHeartbeat – Periodic Heartbeat
	  • processMaxRestartsReached – Process has reached max restart
	  • savedConfigModified – Saved configuration has been modified
	  • serverCertExpired – Server certificate has expired
	  • controllerEvent – Other controller event
	• mobility – Enables mobility traps
	  • operationallyDown – Mobility operationally down
	  • operationallyUp – Mobility operationally up
	  • peerDown – Mobility peer down
	  • peerUp – Mobility peer up

- nsm [dhcpIPChanged] – Enables nsm traps and changes the DHCP IP
- radius-server [radiusServerDown|radiusServerUp] – Enables radius-server traps
  - radiusServerDown – Radius Server is down
  - radiusServerUp – Radius Server is up
- redundancy [adoptionExceeded|criticalResourceDown|criticalResourceUp|grpAuthLevelChanged|memberDown|memberMisConfigured|memberUp] – Enables redundancy traps
  - adoptionExceeded – Redundancy port adoption exceeded
  - criticalResourceDown – Redundancy Critical-Resource Down
  - criticalResourceUp – Redundancy Critical-Resource Up
  - grpAuthLevelChanged – Redundancy group Authorization Level changed
  - memberDown – Redundancy member down
  - memberMisConfigured – Redundancy member mis-configuration
  - memberUp – Redundancy member up
- snmp [authenticationFail|coldstart|linkdown|linkup] – Enables SNMP traps
  - authenticationFail – Enables authentication failure trap
  - coldstart – Enables coldStart trap
  - linkdown – Enables linkDown trap
  - linkup – Enables linkUp trap

- wireless [ap-detection|ids|radio|self-healing|station|wlan] – Enables wireless traps
  - ap-detection [externalAPDetected|externalAPRemoved] – Enables wireless AP detection traps
    - externalAPDetected – Detects an external AP
    - externalAPRemoved – Removes an external AP
  - id [muExcessiveEvents|radioExcessiveEvents|controllerExcessiveEvents] – Enables wireless IDS traps
    - muExcessiveEvents – Excessive and Anomaly Client events
    - radioExcessiveEvents – Excessive radio events
    - controllerExcessiveEvents – Excessive controller events
  - radio [adopted|detectedRadar|unadopted] – Enables wireless radio traps
    - adopted – Radio adopted
    - detectedRadar – Radio detected radar
    - unadopted – Radio unadopted
  - self-healing [activated]– Enables self healing traps
  - station [associated|deniedAssociationAsPortCapacityReached|deniedAssociationOnCapability|deniedAssociationOnErr|deniedAssociationOnInvalidWPAWPA2IE|deniedAssociationOnRates|deniedAssociationOnShortPream|deniedAssociationOnSpectrum|deniedAssociationOnSSID|deniedAuthentication|disassociated |radiusAuthFailed|tkipCounterMeasures|vlanChanged] – Enables wireless station traps

	• associated – Wireless station associated • deniedAssociationAsPortCapacity Reached – Wireless station denied association due to port capacity reached • deniedAssociationOnCapability – Wireless station denied association due to unsupported capability • deniedAssociationOnErr – Wireless station denied association due to internal error • deniedAssociationOnInvalidWPAWPA2IE – Wireless station denied association due to invalid/absent WPA/WPA2 IE • deniedAssociationOnRates – Wireless station denied association due to incompatible Transmission rates • deniedAssociationOnSSID – Wireless station denied association due to invalid SSID • deniedAssociationOnShortPream – Wireless station denied association due to lack of short preamble support • deniedAssociationOnSpectrum – Wireless station denied association due to lack of spectrum management capability • deniedAuthentication – Wireless station denied 802.11 authentication • disassociated – Wireless station disassociated • radiusAuthFailed – Wireless station failed radius authentication • tkipCounterMeasures – TKIP counter measures invoked • vlanChanged – Wireless station vlan id changed
	• wlan [vlanUserLimitReached|webPortalUnavailable|webPortalUnconnected||webPortalUnreachable] – Enables wireless wlan traps when: • vlanUserLimitReached – WLAN-VLAN user limit is reached • webPortalUnavailable – Web portal unavailable • webPortalUnconnected – Web portal disconnected • webPortalUnreachable – Web portal unreachable
password 0 <password>	SMTP Authentication Password. • 0 – Password is specified unencrypted • <password> – Enter password up to 64 characters in length
port <1-65535>	Enter SMTP Server TCP Port.
prefix <smtp-prefix>	Enter SMTP subject prefix up to 16 characters in length.
recipient <1-4> <recipient-address>	Enter SMTP recipient index and SMTP recipient address up to 128 characters in length.
sender <sender-address>	Enter SMTP sender address up to 128 characters in length.
smtp-server-address <IP>	Host to receive SMTP notifications. Enter IP address/Hostname of SNMP server up to 128 characters in length.
user <username>	SMTP Authentication User. Enter username up to 64 characters in length.

Example

```
RFController(config)#smtp-notification enable
RFController(config)#smtp-notification enable traps dhcp-server dhcpServerDown
RFController(config)#snmp-notification recipient 1 admin@serveradmin.com
```

snmp-server

Global Configuration commands

Modifies SNMP engine parameters

Supported in the following platforms:

- Mobility RFS4000 Controller
- Mobility RFS6000 Controller
- Mobility RFS7000 Controller

Syntax

```
snmp-server [community|contact|enable|engine-id|host|
       location|manager|periodic-heartbeat-interval|sysname|user]

snmp-server community <community-string> [ro|rw]
snmp-server contact <contact-person>
snmp-server enable traps {[all|dhcp-server|diagnostics|
       miscellaneous|mobility|nsm|radius-server|redundancy|snmp|
       wireless|wireless-statistics]}
snmp-server enable traps all
snmp-server enable traps dhcp-server {[dhcpServerDown|
       dhcpServerUp]}
snmp-server enable traps diagnostics {[cpuLoad1Min|
       cpuLoad5Min|cpuLoad15Min|fanSpeedLow|fileDescriptors|
       ipRouteCache|packetBuffers|processMemoryUsage|ramFree|
       tempHigh|tempOver|usedKernelBuffer]}
snmp-server enable traps miscellaneous {[caCertExpired|
       lowFsSpace|periodicHeartbeat|processMaxRestartsReached|
       savedConfigModified|serverCertExpired|controllerEvent]}
snmp-server enable traps mobility {[operationallyDown|
       operationallyUp|peerDown|peerUp]}
snmp-server enable traps nsm {dhcpIPChanged}
snmp-server enable traps radius-server
       {[radiusServerDown|radiusServerUp]}
snmp-server enable traps redundancy{[adoptionExceeded|
       criticalResourceDown|criticalResourceUp|
       grpAuthLevelChanged|memberDown|memberMisConfigured|
       memberUp]}
snmp-server enable traps snmp {[authenticationFail|
       coldstart|linkdown|linkup]}
snmp-server enable traps wireless {[ap-detection|ids|
       radio|self-healing|station|wlan]}
snmp-server enable traps wireless ap-detection
       {[externalAPDetected|externalAPRemoved]}
snmp-server enable traps wireless ids
       {[muExcessiveEvents|radioExcessiveEvents|
       controllerExcessiveEvents]}
snmp-server enable traps wireless radio {[adopted|unadopted|detectedRadar]}
snmp-server enable traps wireless self-healing
       activated
snmp-server enable traps wireless station
       {[associated|deniedAssociationAsPortCapacityReached|
       deniedAssociationOnCapability|deniedAssociationOnErr|
       deniedAssociationOnInvalidWPAWPA2IE|
```

```
        deniedAssociationOnRates|deniedAssociationOnShortPream|
        deniedAssociationOnSpectrum|deniedAssociationOnSSID|
        deniedAuthentication|disassociated|radiusAuthFailed|
        tkipCounterMeasures|vlanChanged]}
snmp-server enable traps wireless wlan
        {[vlanUserLimitReached|webPortalUnavailable|
        webPortalUnreachable|webPortalUnconnected]}

snmp-server enable traps wireless-statistics [mesh|
       min-packets|wireless-client|radio|wireless-controller|wlan]
snmp-server enable traps wireless-statistics mesh
        [avg-bit-speed-less-than|avg-retry-greater-than|
        avg-signal-less-than|gave-up-percent-greater-than|
        nu-percent-greater-than|num-wireless-clients-greater-than|
        pktsps-greater-than|tput-greater-than|
        undecrypt-percent-greater-than]
snmp-server enable traps wireless-statistics min-packets
        <1-65535>
snmp-server enable traps wireless-statistics wireless-client
        [avg-bit-speed-less-than|avg-retry-greater-than|
        avg-signal-less-than|gave-up-percent-greater-than|
        nu-percent-greater-than|pktsps-greater-than|
        tput-greater-than|undecrypt-percent-greater-than]
snmp-server enable traps wireless-statistics radio
        [avg-bit-speed-less-than|avg-retry-greater-than|
        avg-noise-level-threshold|avg-signal-less-than|
        gave-up-percent-greater-than|nu-percent-greater-than|
        num-wireless-clients-greater-than|pktsps-greater-than|
        tput-greater-than|undecrypt-percent-greater-than]
snmp-server enable traps wireless-statistics wireless-controller
        [num-wireless-clients-greater-than|pktsps-greater-than|
        tput-greater-than]
snmp-server enable traps wireless-statistics wlan
[avg-bit-speed-less-than|avg-retry-greater-than|
        avg-signal-less-than|gave-up-percent-greater-than|
        nu-percent-greater-than|num-wireless-clients-greater-than|
        pktsps-greater-than|tput-greater-than|
        undecrypt-percent-greater-than]

snmp-server engineid [netsnmp {<word>}|text <word>]
snmp-server host <IP> [v2c|v3] {<1-65535>}
snmp-server location <location-text>
snmp-server manager [all|v2|v3]
snmp-server periodic-heartbeat-interval <interval>
snmp-server sysname

snmp-server user [snmpmanager|snmpoperator|snmptrap]
```

Parameters

community <community-string> [ro|rw]	Sets the community string and access privileges. • <community-string> – Sets the community string • ro – Read-only access with this community string • rw – Read-write access with this community string
contact <contact-person>	Text for mib object sysContact. • <contact-person> – Sets the contact person for this managed node
enable traps *{[all|dhcp-server|diagnostics|miscellaneous|mobility|nsm|radius-server|redundancy|snmp|wireless|wireless-statistics]}*	traps – Enables SNMP traps. All traps are optional. • dhcp-server – Enables dhcp-server traps • diagnostics – Enables diagnostics traps • miscellaneous – Enables miscellaneous traps • mobility – Enables mobility traps • nsm – Enables nsm traps • radius-server – Enables RADIUS server traps • redundancy – Enables redundancy traps • snmp – Enables SNMP traps • wireless – Enables wireless traps • wireless-statistics – Enables wireless statistics traps
enable traps dhcp-server *{[dhcpServerDown|dhcpServerUp]}*	Enables dhcp-server traps. • dhcpServerDown – DHCP server down • dhcpServerUp – DHCP server up
enable traps diagnostics *{[cpuLoad1Min|cpuLoad5Min|cpuLoad15Min|fanSpeedLow|fileDescriptors|ipRouteCache|packetBuffers|processMemoryUsage|ramFree|tempHigh|tempOver|usedKernelBuffer]}*	Enables diagnostics traps. • cpuLoad15Min • cpuLoad1Min • cpuLoad5Min • fanSpeedLow • fileDescriptors • ipRouteCache • packetBuffers • processMemoryUsage • ramFree • tempHigh • tempOver • usedKernelBuffer
enable traps miscellaneous *{[caCertExpired|lowFsSpace|periodicHeartbeat|processMaxRestartsReached|savedConfigModified|serverCertExpired|controllerEvent]}*	Enables miscellaneous traps. • caCertExpired – CA certificate has expired • lowFsSpace – Available file system space is lower than the limit • periodicHeartBeat – Periodic heartbeat trap • processMaxRestartsReached – Process has reached max restart • savedConfigModified – Saved configuration has been modified • serverCertExpired – Server certificate is expired • controllerEvent - Other controller event
enable traps mobility *{[operationallyDown|operationallyUp|peerDown|peerUp]}*	Enable mobility traps. • operationallyDown – Mobility down • operationallyUp – Mobility up • peerDown – Mobility peer down • peerUp – Mobility peer up

enable traps nsm *{dhcpIPChanged}*	Enables nsm traps. • dhcpIPChanged – DHCP IP changed
enable traps radius-server *{[radiusServerDown | radiusServerUp]}*	Enables radius-server traps. • radiusServerDown – RADIUS server down • radiusServerUp – RADIUS server up
enable traps redundancy *{[adoptionExceeded | criticalResourceUp | grpAuthLevelChanged | memberDown | memberMisConfigured | memberUp | criticalResourceDown]}*	Enables redundancy traps. • adoptionExceeded – Redundancy port adoption exceeded • grpAuthLevelChanged – Redundancy group authorization level changed • memberDown – Redundancy member down • memberMisConfigured – Redundancy member mis-configuration • memberUp – Defines redundancy member as up • criticalResourceUp – Critical resource is up • criticalResourceDown – Critical resource is down

enable traps snmp *{[authenticationFail | linkdown | linkup | coldstart]}*	Enables SNMP traps. • authenticationFail – Enables authentication failure trap • coldstart – Enables coldStart trap • linkdown – Enables linkDown trap • linkup – Enables linkUp trap

enable traps wireless *{[ap-detection | ids | radio | self-healing | station | wlan]}*	Enables wireless traps.
	• ap-detection {[externalAPDetected | externalAPRemoved]} – Enables wireless AP detection traps
	  • externalAPDetected – External AP detected
	  • externalAPRemoved – External AP detected
	• ids {[muExcessiveEvents | radioExcessiveEvents | controllerExcessiveEvents]} – Enables wireless IDS traps
	  • muExcessiveEvents – Excessive Client events
	  • radioExcessiveEvents – Excessive radio events
	  • controllerExcessiveEvents – Excessive controller events
	• radio {[adopted | unadopted | detectedRadar]} – Enables wireless radio traps
	  • adopted – Radio adopted
	  • detectedRadar – Radar detected
	  • unadopted – Radio detected radar
	• self-healing activated – Enables self healing traps
	  • activated – Self healing activated
	• station {[associated | deniedAssociationAsPortCapacityReached | deniedAssociationOnCapability | deniedAssociationOnErr | deniedAssociationOnInvalidWPAWPA2IE | deniedAssociationOnRates | deniedAssociationOnShortPream | deniedAssociationOnSpectrum | deniedAssociationOnSSID | deniedAuthentication | disassociated | radiusAuthFailed | tkipCounterMeasures | vlanChanged]} – Enables wireless station traps

	• associated– Wireless station associated • deniedAssociationAsPortCapacityReached – Wireless station denied association - port capacity reached • deniedAssociationOnCapability – Wireless station denied association due to unsupported capability • deniedAssociationOnErr – Wireless station denied association due to internal error • deniedAssociationOnInvalidWPAWPA2IE – Wireless station denied association due to invalid/absent WPA/WPA2 IE • deniedAssociationOnRates – Wireless station denied association due to incompatible Transmission rates • deniedAssociationOnSSID – Wireless station denied association due to invalid SSID • deniedAssociationOnShortPream – Wireless station denied association due to lack of short preamble support • deniedAssociationOnSpectrum – Wireless station denied association due to lack of spectrum management capability • deniedAuthentication – Wireless station denied 802.11 authentication • disassociated – Wireless station disassociated • tkipCounterMeasures – TKIP counter measures invoked • vlanChanged – Wireless station VLAN ID has changed
	• wlan {[vlanUserLimitReached|webPortal Unavailable|webPortalUnreachable|webPortal Unconnected]}– Enables wireless wlan traps • vlanUserLimitReached – WALN/VLAN user limit reached • webPortalUnavailable – Webportal is unavailable • webPortalUnreachable – Webportal is unreachable • webPortalUnconnected – Webportal is not connected

snmp-server enable traps wireless-statistics [mesh| min-packets|wireless-client| radio|wireless-controller|wlan]	Modifies wireless-stats rate traps.
	• mesh [avg-bit-speed-less-than| avg-retry-greater-than|avg-signal-less-than| gave-up-percent-greater-than| nu-percent-greater-than| num-wireless-clients-greater-than| pktsps-greater-than|tput-greater-than| undecrypt-percent-greater-than] – Modifies mesh rate traps
	  • avg-bit-speed-less-than – Average bit speed in Mbps between <0.00> and <54.00>
	  • avg-retry-greater-than – Average retry is greater than 0.00 and less than or equal to 16.00
	  • avg-signal-less-than – Average signal in dBm is less than -0.00 and greater than or equal to -120.00
	  • gave-up-percent-greater-than – Percentage of pkts dropped is greater than 0.00 and less than or equal to 100.00
	  • nu-percent-greater-than – Percentage of non-unicast pkts is greater than 0.00 and less than or equal to 100.00
	  • num-wireless-clients-greater-than – Number of associated wireless-client is <1-8192>
	  • pktsps-greater-than – Packets per sec is greater than 0.00 and less than or equal to 100000.00
	  • tput-greater-than – Throughput in Mbps is greater than 0.00 and less than or equal to 100000.00
	  • undecrypt-percent-greater-than – Percentage of undecryptable pkts is greater than 0.00 and less than or equal to 100.00

	• min-packets <1-65535> – Minimum packets required for sending the trap
	  • <1-65535> – Defines the minimum packets for sending the trap. This can be set with a decimal number in the range of <1-65535>
	• wireless-client [avg-bit-speed-less-than|avg-retry-greater-than|avg-signal-less-than|gave-up-percent-greater-than|nu-percent-greater-than|pktsps-greater-than|tput-greater-than|undecrypt-percent-greater-than] – Modifies wireless-client rate traps
	  • avg-bit-speed-less-than – Average bit speed in Mbps is between <0.00> and <54.00>
	  • avg-retry-greater-than – Average retry is greater than 0.00 and less than or equal to 16.00
	  • avg-signal-less-than – Average signal in dBm is less than -0.00 and greater than or equal to -120.00
	  • gave-up-percent-greater-than – Percentage of pkts dropped is greater than 0.00 and less than or equal to 100.00
	  • nu-percent-greater-than – Percentage of non-unicast pkts is greater than 0.00 and less than or equal to 100.00
	  • pktsps-greater-than – Packets per sec is greater than 0.00 and less than or equal to 100000.00
	  • tput-greater-than – Throughput in Mbps is greater than 0.00 and less than or equal to 100000.00
	  • undecrypt-percent-greater-than – Percentage of undecryptable pkts is greater than 0.00 and less than or equal to 100.00

engineid [netsnmp {<word>}|text <word>]	Sets the SNMP server engine ID. • netsnmp <word>– Sets the engine id to a hexadecimal string • text <word> – Sets the engine id to a text string

host <IP> [v2c|v3] {<1-65535>}	SNMP server host.
	• <IP> – SNMP server host IP address
	  • v2c <1-65535> – Use snmp version 2c
	  • v3 <1-65535> – Use snmp version 3

location <location-text>	Text for mib object sysLocation.
manager [all|v2|v3]	Enables the SNMP manager. • all – Enables SNMP version v2 and v3 • v2 – Enables SNMP version v2 • v3 – Enables SNMP version v3
periodic-heartbeat-interval <interval>	Sets periodic heartbeat trap interval. A periodic trap is sent if no other traps are sent by the controller. The default time period is 60 seconds. Set a value to between 10 and 1000 seconds.

sysname	The SNMP system name.

user [snmpmanager|snmpoperator|snmptrap]	Defines a user who can access the SNMP engine.
	• snmpmanager v3– Manager user
	  • v3 [auth|encrypted] – User using v3 security model
	  • auth md5 <password> – Sets authentication parameters for the user
	  • md5 – Use HMAC MD5 algorithm for authentication
	  • <password> – The password for the user
	  • encrypted [auth|des] – Displays privacy parameters for the user
	  • auth md5 <password>– Displays authentication parameters for the user
	  • des – Use CBC-DES for privacy
	• snmpoperator v3 – Operator user
	• snmptrap v3 – Trap user

Example

```
RFController(config)#snmp-server community TestCommunity ro
RFController(config)#

RFController(config)#snmp-server contact TestManager
RFController(config)#

RFController(config)#snmp-server enable traps all
RFController(config)#

RFController(config)#snmp-server enable traps miscellaneous lowFsSpace
RFController(config)#
RFController(config)#snmp-server enable traps redundancy memberUp
RFController(config)#

RFController(config)#snmp-server enable traps snmp linkup
RFController(config)#

RFController(config)#snmp-server enable traps wireless  ap-detection
externalAPDetected
RFController(config)#

RFController(config)#snmp-server enable traps wireless  ids excessiveProbes
RFController(config)#

RFController(config)#snmp-server enable traps wireless radio adopted
RFController(config)#

RFController(config)#snmp-server enable traps wireless self-healing activated
RFController(config)#

RFController(config)#snmp-server enable traps wireless station
tkipCounterMeasures
RFController(config)#

RFController(config)#snmp-server enable traps wireless-statistics min-packets
120
```

```
RFController(config)#

RFController(config)#snmp-server location "Located at thh 5th FLoor"
RFController(config)#

RFController(config)#snmp-server sysname "Gold Mine"
RFController(config)#

RFController(config)#snmp-server periodic-heartbeat-interval 120
RFController(config)#

RFController(config)#snmp-server engineid netsnmp
RFController(config)#
```

spanning-tree

Global Configuration commands

Configures spanning-tree commands

Supported in the following platforms:

- Mobility RFS4000 Controller
- Mobility RFS6000 Controller
- Mobility RFS7000 Controller

Syntax

```
spanning-tree [mst|portfast]

spanning-tree mst [<0-15> priority <0-61440>|
cisco-interoperability [enable|disable]|configuration|
forward-time <4-30>|hello-time <1-10>|max-age <6-40>|
max-hops <7-127>]

spanning-tree portfast [bpdufilter|bpduguard] default
```

Parameters

mst [<0-15> priority <0-61440>| cisco-interoperability [enable|disable]| configuration| forward-time <4-30>| hello-time <1-10>| max-age <6-40>| max-hops <7-127>]	Enables the Multiple Spanning Tree Protocol on a bridge.
	• <0-15> priority <0-61440> – Set the bridge priority for an MST instance to the value specified. Use the no parameter with this command to restore the default bridge priority value
	  • priority – Sets the bridge priority for the common instance
	  • <0-61440> – Defines the bridge priority in increments of 4096 (Lower priority indicates greater likelihood of becoming root). The default value of the priority for each instance is 32768
	• cisco-interoperability [enable|disable] – Enables/disables interoperability with Cisco's version of MSTP (incompatible with standard MSTP)
	  • enable – Enables CISCO Interoperability
	  • disable – Disables CISCO Interoperability
	• configuration – Multiple spanning tree configuration. This command moves to the **(config-mst)** instance. For more information, see *Chapter 13, Spanning tree-mst Instance*
	• forward-time <4-30> – Sets the time (in seconds) after which (if this bridge is the root bridge) each port changes states to learning and forwarding. This value is used by all instances. The default value is 15 seconds
	• hello-time <1-10> – Sets the hello-time. The hello-time is the time (in seconds) after which (if this bridge is the root bridge) all the bridges in a bridged LAN exchange *Bridge Protocol Data Unit*s (BPDUs). A very low value leads to excessive traffic on the network, while a higher value delays the detection of a topology change. This value is used by all instances. The default value is 2 seconds

	• max-age <6-40> – Max-age is the maximum time in seconds for which (if a bridge is the root bridge) a message is considered valid. This prevents the frames from looping indefinitely. The value of max-age must be greater than twice the value of hello time plus one, but less than twice the value of forward delay minus one. The permissible range for max-age is 6-40 seconds. Configure this value sufficiently high, so a frame generated by root can be propagated to the leaf nodes without exceeding the max-age. Use this command to set the max-age for a bridge. This value is used by all instances.The default value of bridge max-age is 20 seconds • max-hops <7-127> – Specifies the maximum allowed hops for a BPDU in an MST region. This parameter is used by all MST instances. To restore the default value, use the no parameter with this command. The default maxhops in a MST region is 20
portfast [bpdufilter|bpduguard] default	Enables the portfast feature on a bridge. It has the following options: • bpdufilter default – Use the `bpdu-filter` command to set the portfast BPDU filter for the port. Use the `no` parameter with this command to revert the port BPDU filter value to default. The Spanning Tree Protocol sends BPDUs from all ports. Enabling the BPDU Filter feature ensures PortFastenabled ports do not transmit or receive BPDUs • bpduguard default – Use the `bpdu-guard` command to enable the BPDU (Bridge Protocol Data Unit) Guard feature on a bridge. Use the `no` parameter with this command to disable BPDU Guard. When the BPDU Guard is set for a bridge, all portfast-enabled ports of the bridge that have BPDU guard set to default shut down the port on receiving a BPDU. In this case, the BPDU is not processed. The port can be brought back up manually (using the no shutdown command), or by configuring a errdisable-timeout to enable the port after the specified interval

Usage Guidelines

The `mst > configuration` command moves you to the *Spanning tree-mst Instance on page 435* Instance instance.

If a bridge does not hear bridge protocol data units (BPDUs) from the root bridge within the specified interval, defined in the max-age (seconds) parameter, assume the network has changed and recomputed the spanning-tree topology.

Generally, spanning tree configuration settings in the config mode define the configuration for bridge and bridge instances.

Example

```
RFController(config)#spanning-tree portfast bpduguard default
RFController(config)#

RFController(config)#spanning-tree mst configuration
RFController(config-mst)#
```

timezone

Global Configuration commands

Configures controller timezone settings

Supported in the following platforms:

- Mobility RFS4000 Controller
- Mobility RFS6000 Controller
- Mobility RFS7000 Controller

Syntax

```
timezone <timezone>
```

Parameters

<timezone>	Press <tab> to traverse a list of files. This displays a list of files containing timezone information.

Example

```
RFController(config)#timezone
Africa/     America/    Asia/       Atlantic/   Australia/  CET
CST6CDT     EET         Etc/        Europe/     MST7MDT     Pacific/
PST8PDT     EST5EDT
RFController(config)#timezone

RFController(config)#timezone America/
America/Anchorage     America/Bogota        America/Buenos_Aires
America/Caracas       America/Chicago
America/Costa_Rica    America/Denver        America/Los_Angeles
America/Mexico_City   America/Montreal
America/New_York      America/Phoenix       America/Santiago
America/Sao_Paulo     America/St_Johns
America/Tegucigalpa   America/Thule         America/Winnipeg
America/Indianapolis

RFController(config)#timezone America/Chicago
RFController(config)#
```

traffic-shape

Global Configuration commands

Optimizes network traffic

Supported in the following platforms:

- Mobility RFS7000 Controller

NOTE
This command is not supported on the Mobility RFS4000 Controller and on the Mobility RFS6000 Controller.

Syntax

```
traffic-shape [class|priority-map]
traffic-shape class <class-identifier> [max-buffers|
       max-latency|rate]
traffic-shape class <class-identifier> max-buffers
       <pri0-queue-length> <pri1-queue-length>
       <pri2-queue-length> <pri3-queue-length>
       <pri4-queue-length> <pri5-queue-length>
       <pri6-queue-length> <pri7-queue-length> red-level
       <pri0-queue-length-for-red> <pri1-queue-length-for-red>
       <pri2-queue-length-for-red> <pri3-queue-length-for-red>
       <pri4-queue-length-for-red> <pri5-queue-length-for-red>
       <pri6-queue-length-for-red> <pri7-queue-length-for-red>
traffic-shape class <class-identifier> max-buffers
       <pri0-queue-length> <pri1-queue-length>
       <pri2-queue-length> <pri3-queue-length>
       <pri4-queue-length> <pri5-queue-length>
       <pri6-queue-length> <pri7-queue-length> red-percent
       <pri0-queue-percent-for-red> <pri1-queue-percent-for-red>
       <pri2-queue-percent-for-red> <pri3-queue-percent-for-red>
       <pri4-queue-percent-for-red> <pri5-queue-percent-for-red>
       <pri6-queue-percent-for-red> <pri7-queue-percent-for-red>
traffic-shape class <class-identifier> max-latency
       <pri0-queue-latency> <pri1-queue-latency>
       <pri2-queue-latency> <pri3-queue-latency>
       <pri4-queue-latency> <pri5-queue-latency>
       <pri6-queue-latency> <pri7-queue-latency> [msec|usec]
traffic-shape class <class-identifier> rate {[Kbps|Mbps|bps]}

traffic-shape priority-map <0-7> <0-7> <0-7> <0-7> <0-7> <0-7> <0-7> <0-7>
```

Parameters

class <class-identifier> max-buffers ... red-level ...
class <class-identifier> max-buffers ... red-percent ...
class <class-identifier> max-latency ... [msec|usec]
class <class-identifier> rate *{[Kbps|Mbps|bps]}*
	Traffic shaping packet class. Select an identifier between 1-4. Traffic shaping also uses queues numbered 0-7.
	• max-buffers – Maximum traffic-shape queue length in packets
	  • <1-2000> – Maximum length of lowest or all priority queues
	  • red-level – Performs RED (random early drop) when the queue length is reached
	  • red-percent – Performs RED (random early drop) at a percentage of max-buffers
	• max-latency – Maximum packet delay in queue
	  • <1-1000000> – Maximum latency of lowest or all priority queues
	  • [msec|usec] – Sets the time measure
	• rate <1-250000000> – Traffic rate (250 Kbps-250 Mbps)
	  • Kbps – Units of kilobits/sec
	  • Mbps – Units of megabits/sec
	  • bps – Units of bits/sec

priority-map <0-7> <0-7> ...	Sets 802.1p to priority queue maps for all the traffic shape queues.

Example

```
RFSController(config)#traffic-shape class 1 max-buffers 1000 1000 1000 1000
500 500 500 500 red-level 750 750 750 750 375 375 375 375
RFSController(config)#traffic-shape class 1 max-latency 1000 1000 1000 1000
1000 1000 1000 1000 msec
RFSController(config)#traffice-shape class 1 rate 100000 Kbps
RFSController(config)#traffic-shape priority-map 1 2 0 7 5 3 6 4
RFSController(config)#show  traffic-shape config

Traffic shaping class 1
   Rate: 10 Mbps
   Prio-|  max |     RED     | max
   rity | pkts | pkts pcnt | latency
      0 | 1000 |  750  75% | -
      1 | 1000 |  750  75% | -
      2 | 1000 |  750  75% | -
      3 | 1000 |  750  75% | -
      4 |  500 |  375  75% | -
      5 |  500 |  375  75% | -
      6 |  500 |  375  75% | -
      7 |  500 |  375  75% | -
Traffic shaping class 2
   Not configured
Traffic shaping class 3
   Not configured
Traffic shaping class 4
   Not configured
RFController(config)#show traffic-shape priority-map
 802.1p | Shaping priority
     0  |  1
     1  |  2
     2  |  0
     3  |  7
     4  |  5
```

5	3
6	6
7	4

username

Global Configuration commands

Establishes user name authentication

Supported in the following platforms:

- Mobility RFS4000 Controller
- Mobility RFS6000 Controller
- Mobility RFS7000 Controller

Syntax

```
username <name> [access|password|privilege]
username <name> access [console|ssh|telnet|web]
username <name> password [0 <password>|1 <password>|
       <password>]
username <name> privilege [helpdesk|monitor|nwadmin|
       superuser|sysadmin|webadmin]
```

Parameters

<name>	Enter a name to authenticate the controller, the username should be between 1 and 28 characters.
	• access [console|ssh|telnet|web]– Sets the user access mode
	  • console – Only allowed from console
	  • ssh – Only allowed from ssh
	  • telnet – Only allowed from telnet
	  • web – Only allowed from applet (webUI)
	• password [0 <password>|1 <password>|<password>] – Specifies the password for the user
	  • 0 – Password is specified UNENCRYPTED
	  • 1 – Password is encrypted with SHA1 algorithm
	  • <password> – User password
	  • *plaintext* password length should be between 8 and 32 letters
	  • *encrypted* password length should be 40 letters)

	• privilege [helpdesk|monitor|nwadmin|superuser|sysadmin|webadmin] – Sets user access privilege
	  • helpdesk – Helpdesk (troubleshooting) access
	  • monitor – Monitor (read-only) access
	  • nwadmin – Network (wired & wireless) admin access
	  • superuser – Superuser (root) access
	  • sysadmin – System (general system configuration) admin access
	  • webadmin – Web auth (hotspot) user admin access

Example

```
RFController(config)#username GoldenController
RFController(config)#

RFController(config)#username Aeyjey access console ssh telnet web
RFController(config)#username JohnDoe privilege sysadmin webadmin nwadmin
```

Encrypting a Password

To encrypt a password:

1. Enable password encryption and provide the passphrase required for encrypting the passwords.

```
RFController(config)#service password-encryption secret 2 Brocade
RFController(config)#username Jiri password admin
```

2. On completion of the above step, all the passwords, crypto keys, shared secrets etc are displayed in an encrypted format in the running/startup configuration.

```
RFController(config)#show run
!
! configuration of Mobility RFS6000 Controller version 4.2.1.0
!
version 1.1
!
!
aaa authentication login default none
service prompt crash-info
!


username admin password 1 8e67bb26b358e2ed20fe552ed6fb832f397a507d
username admin privilege  superuser

username operator password 1    fe96dd39756ac41b74283a9292652d366d73931f

username Jiri password 1 399f01e13e372ba2dc02f37d869021873e60aa85
```

3. The password in the above running configuration is displayed in an encrypted format even though it was entered as plain text in Step 1.

vpn

Global Configuration commands

Configures VPN authentication settings

Supported in the following platforms:

- Mobility RFS4000 Controller
- Mobility RFS6000 Controller
- Mobility RFS7000 Controller

Syntax

```
vpn authentication-method [local|radius]
```

Parameters

authentication-method [local|radius]	Selects the authentication scheme. • local – Used for user based authentication • radius – Used for RADIUS server authentication

Usage Guidelines

Virtual Private Network (VPN) enables IP traffic to travel securely over a public TCP/IP network by encrypting all traffic from one network to another. A VPN uses "tunneling" to encrypt all information at the IP level.

wireless

Global Configuration commands

Configures controller wireless parameters

This command moves you to the `config-wireless` instance. For more information, see *Chapter 20, Wireless Instance*.

Supported in the following platforms:

- Mobility RFS4000 Controller
- Mobility RFS6000 Controller
- Mobility RFS7000 Controller

Syntax

```
wireless
```

Parameters

None

Usage Guidelines

The wireless command is used to enter the config-wireless instance wherein you can configure wireless parameters. Confirm you have entered the wireless instance, as the prompt changes from the regular `RFController(config)#` to `RFController(config-wireless)#`.

Example

```
RFController(config)#wireless
RFController(config-wireless)#
```

wlan-acl

Global Configuration commands

Applies an ACL on a WLAN index

Supported in the following platforms:

- Mobility RFS4000 Controller
- Mobility RFS6000 Controller
- Mobility RFS7000 Controller

Syntax

```
wlan-acl <1-256> [<1-99>|<100-199>|<1300-1999>|
       <2000-2699>|<acl-name>] [in|out]
```

Parameters

<1-32>	WLAN number
[<1-99>|<100-199>|<1300|1999>|<2000|2699>|word]	• <1-99> — IP standard access list • <100-199> — IP extended access list • <1300-1999> — IP standard access list (expanded range) • <2000-2699> — IP extended access list (expanded range) • <acl-name> — Access list name
[in|out]	• in — Incoming packets • out — Outgoing packets

Usage Guidelines 1

Every WLAN created is mapped to an index. When an ACL is applied on a WLAN index it becomes a WLAN ACL. The following type of ACL's can be applied on a WLAN:

- IP Standard ACL
- IP Extended ACL
- MAC Extended ACL

When a packet is sent from a client to a WLAN index of an access point, it becomes an inbound traffic to the wireless LAN.

When a packet goes out of a access point, it becomes outbound traffic to the wireless LAN index. Apply an ACL to a WLAN index in outbound direction to filter traffic from both wired and wireless interfaces.

`wlan-acl` can be attached both in the inbound and outbound directions.

NOTE
Most of the Wireless LAN related configuration are performed using the *Chapter 20, Wireless Instance*. Use `wlan-acl` (in the global configuration mode) to apply an ACL on a wireless LAN index .

The last ACE in the access list is an implicit deny statement. Whenever the interface receives the packet, its content is checked against all the ACE's in the ACL. It is allowed/denied based on the ACL configuration.

NOTE
All ACLs which had WLAN index are now replaced with ones that don't have WLAN index.
In the above process, the acl "110" had two rules which got replaced by only one rule because after removal of WLAN index selector, both the rules look similar.

Follow the procedure below to manually upgrade the ACLs to the same configuration:

1. If all the rules in ACL have same WLAN index as **selector** and there are no other ACL rules, then attach the ACL to the WLAN port.

   In the above example, the ACL "**macacl**" has two rules for WLAN 14 which can be attached to WLAN port as follows:

   ```
   wlan-acl 14 macacl in
   ```

2. If the ACL has mix of rules – with different WLAN indices and without an WLAN indices, it should be grouped as follows:
   a. Create separate ACLs for all rules with a given WLAN index.
   b. Create separate ACLs for rules which do not have any WLAN index.

To manually configure a Standard ACL, the example above has to be split into 3 ACLs.

```
ip access-list standard stdacl1
permit any rule-precedence 34

ip access-list standard stdacl2
permit host 10.0.0.10 rule-precedence 44

ip access-list standard stdacl3
deny host 30.0.0.14 rule-precedence 54

no access-list stdacl

wlan-acl 5 stdacl1 in

wlan-acl 6 stdacl2 in
```

The stdacl must be detached from the interface to which it was associated and stdacl3 must be attached to that interface.

When the user explicitly creates ACL rules with WLAN index as selector, the controller consumes that ACL without WLAN index selector. During this process a warning is raised to the user as mentioned in the example below.

```
RFController(config)#access-list 14 permit any wlan 19 log
Warning : Acl rules with Wlan Index is deprecated. Wlan index configured for
the rule will be ignored. Please use wlan-acl CLI to apply ACLs on WLAN
```

Example

The example below applies an ACL to WLAN index 200 in an inbound direction from the global config mode.

```
RFController(config)#wlan-acl 2 150 in
RFController(config)#
```

NOTE
A MAC access list entry to allow `arp` is mandatory to apply an IP based ACL to an interface. MAC ACL always takes precedence over IP based ACL's.

The example below applies an ACL to WLAN index 200 in outbound direction from the global config mode.

```
RFController(config)#wlan-acl 2 150 out
RFController(config)#
```

network-element-id

Global Configuration commands

Use this command to set system's network-element-ID

Supported in the following platforms:

- Mobility RFS4000 Controller
- Mobility RFS6000 Controller
- Mobility RFS7000 Controller

Syntax

```
network-element-id <element-id>
```

Parameters

<element-id>	Specifies system's network element ID

Example

```
RFController(config)#network-element-id test
RFController(config)#
```

firewall

Global Configuration commands

Use this command to set system's network-element-ID

Supported in the following platforms:

- Mobility RFS4000 Controller
- Mobility RFS6000 Controller
- Mobility RFS7000 Controller

Syntax

```
firewall
[802.2-encapsulation|dhcp-snoop-conflict-detection|dhcp-snoop-conflict-loggin
g|clamp|enable|flow|virtual-defrag|vlan-stacking]

firewall enable
firewall 802.2-encapsulation permit
firewall clamp [path-mtu|tcp-mss]

firewall flow timeout [icmp|other|tcp|udp]
firewall flow timeout [icmp|other|udp] <10-32400>
firewall flow timeout tcp [close-wait|established|reset|
       setup] <10-32400>

firewall virtual-defrag [enable|max-defrag-per-host|
       max-frags-per-dgram|min-1st-frag-length]
firewall virtual-defrag enable
firewall virtual-defrag max-defrag-per-host <1-32>
firewall virtual-defrag max-frags-per-dgram <2-8129>
firewall virtual-defrag min-1st-frg-length <8-1500>

firewall vlan-stacking permit
```

Parameters

enable	Enables the firewall for this controller.
802.2.-encapsulation permit	Sets 802.2 packet encapsulation. • permit – Allow 802.2 packet encapsulations which can bypass the firewall. Enabling this option is not recommended by Brocade

clamp [path-mtu|tcp-mss]	Configures wireless firewall
	• clamp [path-mtu|tcp-mss] – Displays clamp value
	  • path-mtu – Displays limit discovered path-mtu
	  • tcp-mss – Displays limit TCP to inner path-mtu

flow timeout [icmp|other|tcp|udp]	Configures firewall flow of packets.
	• timeout [icmp|other|udp] <1-32400> – Sets the timeout value for type ICMP, UDP, and Other to a value between 1 and 32400 seconds
	• timeout tcp [close-wait|established|reset|setup] <10-32400> – Sets the timeout value for TCP packet types to a value between 1 and 32400 seconds
	  • close-wait – Configures the Closed TCP Flow timeout value
	  • established – Configures the Established TCP Flow timeout value
	  • reset – Configures the Reset TCP Flow timeout value
	  • setup – Configures the Opening TCP Flow timeout value

virtual-defrag [enable|max-defrag-per-host|max-frags-per-dgram|min-1st-frag-length]	Configures IPv4 virtual defragmentation. • enable – enables IPv4 virtual defragmentation. Brocade recommends that this option be enabled • max-defrag-per-host <1-32> – Sets the maximum active defragmentation per host to a value between 1 and 32 • max-frags-per-dgram <2-8129> – Sets the maximum allowed fragmentation per datagram to a value between 2 and 8129 • min-1st-frag-len < <8-1500> – Sets the minimum fragmentation length for the 1st fragment to a value between 8 and 1500
vlan-stacking permit	Configures 802.1q VLAN stacking. • permit – Permits 802.1q VLAN stacking that can bypass the firewall. Brocade does not recommend the use of this option

Example

```
RFController(config)#firewall clamp
RFController(config)#
```

virtual-ip

Global Configuration commands

Displays virtual-ip configuration of the controller

Supported in the following platforms:

- Mobility RFS4000 Controller
- Mobility RFS6000 Controller
- Mobility RFS7000 Controller

Syntax

```
virtual-ip [<A.B.C.D/M>|advt-timeout <1-5>|enable|
garp-timeout <30-600>|learning-timeout <2-5>|priority|vmac]
virtual-ip <A.B.C.D/M> vlan <1-4096>
virual-ip priority [<1-256>|auto]
virual-ip vmac <AA-BB-CC-DD-EE-FF>
```

Parameters

<A.B.C.D/M> vlan <1-4096>	Displays virtual-ip configuration details of the controller • <A.B.C.D/M> – Displays ip address of the controller • vlan <1-4096> – Displays vlan of the vip • <1-4096> – Displays the vlan range value of the vip
advt-timeout <1-5>	Displays advertisement timeout in seconds • <1-5> – Displays the value in seconds
enable	Enables IP Redundancy protocol
garp-timeout <30-600>	Displays Gratituous ARP timeout in seconds . The default time is 180 seconds • <30-600> – Displays value in seconds
learning-timeout <2-5>	Displays learning timeout in seconds • <2-5> – Displays learning timeout value in seconds
priority [<1-256>|auto]	Displays priority of the controller • <1-256> – Displays manual priority range • auto – Displays automatic priority selection
vmac <AA-BB-CC-DD-EE-FF>	Virtual MAC to be used by the master • <AA-BB-CC-DD-EE-FF> – Allowed VMACs: from 00:15:70:88:8a:90 to 00:15:70:88:8b:8f

Example

```
RFController(config)#virtual-ip 192.168.11.10/24 vlan 11
RFController(config)#
RFController(config)#show virtual-ip config
VIP Status                    : Disabled
Cluster Redundancy Status     : Enabled
Priority Selection Mode       : Automatic
VMAC Selection Mode           : Automatic
Learning Timeout(sec)         : 2
Advertisement Timeout(sec)    : 1
External VLAN                 : 0
External Gateway              : 0.0.0.0
Virtual-IP Server Port        : 51525
```

```
Controller IP               : 192.168.11.4
Controller Id               : 192.168.11.4
Reserved VMAC Address Range : 00-15-70-88-8A-90 to 00-15-70-88-8B-8F
DHCP Server status          : Not Running on this Controller
=================================================================
Vlan | Priority | ControllerID | VIP           |  VMAC
=================================================================
11 | 3232238340 | 192.168.11.4 | 192.168.11.10 | 00-15-70-88-8A-90
=================================================================
RFController(config)#
#
RFController(config)#virtual-ip vmac 00-15-70-88-8A-90
RFController(config)#virtual-ip priority auto
```

wwan

Global Configuration commands

Configures wireless wan interface

Supported in the following platforms:

- Mobility RFS4000 Controller
- Mobility RFS6000 Controller

NOTE
This command is not supported on the Mobility RFS7000 Controller.

Syntax

```
wwan [apn<STRING>|disable|enable|password<STRING>
|username<STRING>]
```

Parameters

apn <STRING>	Enter the access point name provided by the service provider. <STRING> – A string of up to 25 characters **NOTE:** Use this command for countries in Europe. This command is not valid for other countries.
disable	Disables the wireless wan feature
enable	Enables the wireless wan feature
password <STRING>	Enter password provided by the service provider <STRING> – A string of up to 30 characters
username <STRING>	Enter username provided by the service provider <STRING> – A string of up to 32 characters

Example

```
RFController(config)#wwan disable
RFController(config)#

RFController(config)#no wwan apn
RFController(config)#
```

aap-wlan-acl

Global Configuration commands

Applies an acl on wlan for aap

Supported in the following platforms:

- Mobility RFS4000 Controller
- Mobility RFS6000 Controller
- Mobility RFS7000 Controller

Syntax

```
aap-wlan-acl <1-256> [<100-199>|<WORD>]{in/out}
```

Syntax (Mobility RFS6000 Controller)

```
aap-wlan-acl <1-32>[<100-199>|<WORD>]{in/out}
```

Parameters

aap-wlan-acl <1-256> [<100-199>| <WORD>{in|out}	Applies an acl on wlan for an aap <1-256> – Displays wlan index <100-199> Displays IP extended access list WORD> – Displays access list name in – Displays incoming packets out – Displays outgoing packets

Example

```
RFController(config)#aap-wlan-acl 6 symbol in
RFController(config)#

RFController(config)#aap-wlan-acl 6 125 out
RFController(config)#
```

arp

Global Configuration commands

Configures Address Resolution Protocol

Supported in the following platforms:

- Mobility RFS4000 Controller
- Mobility RFS6000 Controller
- Mobility RFS7000 Controller

Syntax

```
arp [<WORD>|ge <1-5>|sa <1-6>|up1|vlan <1-4094|
wwan]{<AB.C.D> <AA-BB-CC-DD-EE-FF>}
```

Parameters

arp [<WORD>|ge <1-5>|sa <1-6>|up1|vlan <1-4094| wwan] {<AB.C.D> <AA-BB-CC-DD-EE-FF>}	Configures address resolution protocol. • <WORD> – Configures interface name • ge <1-5> – Configures Gigabit Ethernet interface • sa <1-6> – Configures Static Aggregate interface • up1 – Configures WAN interface • vlan <1-4094> – Configures vlan • wwan – Configures wireless WAN interface The following parameters are common for all the above. • <A.B.C.D> – Displays Internet Protocol • <AA-BB-CC-DD-EE-FF> – Displays MAC address

Example

```
RFController(config)# arp ge 2 1.2.3.4 11-22-33-44-55-66
RFController(config)
```

power

Global Configuration commands

Configures PoE commands

Supported in the following platforms:

- Mobility RFS4000 Controller
- Mobility RFS6000 Controller

NOTE
This command is not supported on the Mobility RFS7000 Controller.

Syntax

```
power trap-percent <0-100>
```

Parameters

power trap-percent <0-100>	Configures PoE commands trap-percent <0-100> – Configures PoE traps <0-100> – Percentage of total power at which trap is generated

Example

```
RFController(config)#power trap-percent 99
RFController(config)#
```

aap-ipfilter-list

Global Configuration commands

Applies ipfilter to WLAN/LAN

Supported in the following platforms:

- Mobility RFS4000 Controller
- Mobility RFS6000 Controller
- Mobility RFS7000 Controller

NOTE
aap-ipfilter-list command initiates (config-aap-ip-filter-list) instance. For more details see *Chapter 27, AAP IP Filtering*. The prompt changes from `RFController (config)#` to `RFController (config-aap-ipfilter).`

Parameters

```
aap-ipfilter-list
```

Parameters

None

Example

```
RFController(config)#aap-ipfilter-list
RFController(config-aap-ipfilter)#
```

whitelist

Global Configuration commands

White list is a list of host names and IP addresses that are permitted access by default.

Supported in the following platforms:

- Mobility RFS4000 Controller
- Mobility RFS6000 Controller
- Mobility RFS7000 Controller

NOTE
whitelist command instantiates (config-whitelist) instance. The prompt changes from `RFController (config)#` to `RFController (config-whitelist)`

Syntax

```
whitelist [clrscr|end|exit|help|no|permit|show|service]
whitelist no permit
whitelist permit [<A.B.C.D>|<Hostname>]
```

Parameters

clrscr	Clears the display screen.
end	Ends the current mode and changes to EXEC mode.
exit	Ends the current mode and changes to previous mode.
help	Displays the interactive help system.
no	Negates a command or sets its defaults.
[<A.B.C.D>|Hostname <suffix>]	Permits list of hostnames and IP addresses. <A.B.C.D> – Displays IP address <Hostname> suffix – Displays hostname suffix – Matches any hostname including this one as suffix

Example

```
RFController(config-whitelist)#permit 172.16.10.3
RFController(config-whitelist)#permit brocade suffix
RFController(config-whitelist)#
```

Chapter

Crypto-isakmp Instance

6

In this chapter

The `(config-crypto-isakmp)` instance is used to configure ISAKMP policies. To enter this instance, use this command:

```
RFController(config)#crypto isakmp policy <1-10000>
RFController(config-crypto-isakmp)#
```

Crypto ISAKMP config commands

Table 6 summarizes **`crypto-isakmp`** commands

TABLE 6 Crypto-isakmp Instance

Command	Description	Ref.
authentication	Sets the authentication scheme	*page 328*
clrscr	Clears the display screen	*page 329*
encryption	Sets the encryption algorithm	*page 330*
end	Ends the current mode and moves to the EXEC mode	*page 331*
exit	Ends the current mode and moves to the previous mode	*page 332*
group	Sets the Diffie-Hellman group	*page 333*
hash	Sets the hash algorithm	*page 334*
help	Provides a description of the interactive help system	*page 335*
lifetime	Sets the lifetime for the ISAKMP security association	*page 336*
no	Negates a command or sets its defaults	*page 337*
service	Defines the controllers service commands	*page 338*
show	Shows running system information	*page 339*

authentication

Crypto ISAKMP config commands

Authenticates rsa-sig and pre-share keys

Supported in the following platforms:

- Mobility RFS4000 Controller
- Mobility RFS6000 Controller
- Mobility RFS7000 Controller

Syntax

```
authentication [pre-share|rsa-sig]
```

Parameters

pre-share	pre shared key
rsa-sig	rsa signature

Example

```
RFController(config-crypto-isakmp)#authentication pre-share
RFController(config-crypto-isakmp)#

RFController(config-crypto-isakmp)#authentication rsa-sig
RFController(config-crypto-isakmp)#
```

clrscr

Crypto ISAKMP config commands

Clears the display screen

Supported in the following platforms:

- Mobility RFS4000 Controller
- Mobility RFS6000 Controller
- Mobility RFS7000 Controller

Syntax

```
clrscr
```

Parameters

None.

Example

```
RFController(config-crypto-isakmp)#clrscr
RFController(config-crypto-isakmp)#
```

encryption

Crypto ISAKMP config commands

Configures the encryption level of the data transmitted using the `crypto-isakmp` command

Supported in the following platforms:

- Mobility RFS4000 Controller
- Mobility RFS6000 Controller
- Mobility RFS7000 Controller

Syntax

```
encryption [3des|aes|aes-192|aes-256|des]
```

Parameters

3des	Triple data encryption standard
aes	Advanced data encryption standard
aes-192	Advanced data encryption standard
aes-256	Advanced data encryption standard
des	Data encryption standard

Example

```
RFController(config-crypto-isakmp)#encryption 3des
RFController(config-crypto-isakmp)#

RFController(config-crypto-isakmp)#encryption aes-256
RFController(config-crypto-isakmp)#
```

end

Crypto ISAKMP config commands

Ends and exits the current mode and changes to the PRIV EXEC mode. The prompt changes to `RFController#`

Supported in the following platforms:

- Mobility RFS4000 Controller
- Mobility RFS6000 Controller
- Mobility RFS7000 Controller

Syntax

```
end
```

Parameters

None.

Example

```
RFController(config-crypto-isakmp))#end
RFController#
```

exit

Crypto ISAKMP config commands

Ends the current mode and moves to the previous mode (GLOBAL-CONFIG). The prompt changes to `RFController(config)#`

Supported in the following platforms:

- Mobility RFS4000 Controller
- Mobility RFS6000 Controller
- Mobility RFS7000 Controller

Syntax

```
exit
```

Parameters

None.

Example

```
RFController(config-crypto-isakmp)#exit
RFController(config)#
```

group

Crypto ISAKMP config commands

Specifies the Diffie-Hellman group (1 or 2) used by the IKE policy to generate keys (which is then used to create an IPSec SA)

Supported in the following platforms:

- Mobility RFS4000 Controller
- Mobility RFS6000 Controller
- Mobility RFS7000 Controller

Syntax

```
group [1|2|5]
```

Parameters

1	Diffie-Hellman group 1
2	Diffie-Hellman group 2
5	Diffie-Hellman group 5

Usage Guidelines

The local IKE policy and the peer IKE policy must have matching group settings in order for negotiation to be successful.

Example

```
RFController(config-crypto-isakmp)#group 5
RFController(config-crypto-isakmp)#
```

hash

Crypto ISAKMP config commands

Specifies the hash algorithm used to authenticate data transmitted over the IKE SA

Supported in the following platforms:

- Mobility RFS4000 Controller
- Mobility RFS6000 Controller
- Mobility RFS7000 Controller

Syntax

```
hash [md5|sha]
```

Parameters

md5	Choose the MD5 hash algorithm
sha	Choose the SHA hash algorithm

Example

```
RFController(config-crypto-isakmp)#hash sha
RFController(config-crypto-isakmp)#
```

help

Crypto ISAKMP config commands

Displays the system's interactive help system

Supported in the following platforms:

- Mobility RFS4000 Controller
- Mobility RFS6000 Controller
- Mobility RFS7000 Controller

Syntax

```
help
```

Parameters

None.

Example

```
RFController(config-crypto-isakmp)#help
CLI provides advanced help feature.  When you need help,
anytime at the command line please press '?'.

If nothing matches, the help list will be empty and you must backup
until entering a '?' shows the available options.
Two styles of help are provided:
1. Full help is available when you are ready to enter a
   command argument (e.g. 'show ?') and describes each possible
   argument.
2. Partial help is provided when an abbreviated argument is entered
   and you want to know what arguments match the input
   (e.g. 'show ve?'.)
RFController(config-crypto-isakmp)#
```

lifetime

Crypto ISAKMP config commands

Specifies how long an IKE SA is valid before it expires

Supported in the following platforms:

- Mobility RFS4000 Controller
- Mobility RFS6000 Controller
- Mobility RFS7000 Controller

Syntax

```
lifetime <seconds>
```

Parameters

<seconds>	Specifies how many seconds an IKE SA lasts before it expires. A time stamp (in seconds) can be configured between 60 and 2147483646.

Example

```
RFController(config-crypto-isakmp)#lifetime 5200
RFController(config-crypto-isakmp)#
```

no

Crypto ISAKMP config commands

Negates a command or sets its defaults

Supported in the following platforms:

- Mobility RFS4000 Controller
- Mobility RFS6000 Controller
- Mobility RFS7000 Controller

Syntax

```
no [authentication|encryption|group|hash|lifetime]
```

Parameters

None.

Example

```
RFController(config-crypto-isakmp)#no lifetime
RFController(config-crypto-isakmp)#
```

service

Crypto ISAKMP config commands

Invokes service commands to troubleshoot or debug the `(config-crypto-isakmp)` instance configurations.

Supported in the following platforms:

- Mobility RFS4000 Controller
- Mobility RFS6000 Controller
- Mobility RFS7000 Controller

Syntax

```
service show cli
```

Parameters

cli	Displays the CLI tree of current mode

Example

```
RFController(config-crypto-isakmp)#service show cli
Crypto Isakmp Config mode:
+-authentication
  +-pre-share [authentication ( rsa-sig | pre-share )]
  +-rsa-sig [authentication ( rsa-sig | pre-share )]
+-clrscr [clrscr]
+-do
  +-LINE [do LINE]
+-encryption
  +-3des [encryption ( des | 3des | aes | aes-192 | aes-256 )]
  +-aes [encryption ( des | 3des | aes | aes-192 | aes-256 )]
  +-aes-192 [encryption ( des | 3des | aes | aes-192 | aes-256 )]
  +-aes-256 [encryption ( des | 3des | aes | aes-192 | aes-256 )]
  +-des [encryption ( des | 3des | aes | aes-192 | aes-256 )]
+-end [end]
+-exit [exit]
+-group
  +-1 [group (1|2|5)]
  +-2 [group (1|2|5)]
  +-5 [group (1|2|5)]
+-hash
  +-md5 [hash (sha|md5)]
.................

RFController(config-crypto-isakmp)#
```

show

Crypto ISAKMP config commands

Displays current system information running on the controller

Supported in the following platforms:

- Mobility RFS4000 Controller
- Mobility RFS6000 Controller
- Mobility RFS7000 Controller

NOTE
The following commands display only for the Mobility RFS6000 Controller and the Mobility RFS4000 Controller
- power
The following commands display only for the Mobility RFS7000 Controller and the Mobility RFS4000 Controller:
- port-channel
- static-channel-group

NOTE
For more details, see *show on page 59*

Syntax

```
show <paramater>
```

Parameters

?	Displays all the parameters for which information can be viewed using the show command

Example

```
RFController(config-crypto-isakmp)#show ?
  access-list           Internet Protocol (IP)
  aclstats              Show ACL Statistics information
  alarm-log             Display all alarms currently in the system
  autoinstall           autoinstall configuration
  banner                Display Message of the Day Login banner
  boot                  Display boot configuration.
  clock                 Display system clock
  commands              Show command lists
  crypto                encryption module
  debugging             Debugging information outputs
  dhcp                  DHCP Server Configuration
  environment           show environmental information
  file                  Display filesystem information
  firewall              Wireless firewall
  ftp                   Display FTP Server configuration
  history               Display the session command history
  interfaces            Interface status
  ip                    Internet Protocol (IP)
  ldap                  LDAP server
  licenses              Show any installed licenses
  logging               Show logging configuration and buffer
```

```
  mac                   Internet Protocol (IP)
  mac-address-table     Display MAC address table
  mac-name              Displays the configured MAC names
  management            Display L3 Managment Interface name
  mobility              Display Mobility parameters
  ntp                   Network time protocol
  password-encryption   Password encryption
  port                  Physical/Aggregate port interface
  port-channel          Portchannel commands
  privilege             Show current privilege level
  protocol-list         List of protocols
  radius                RADIUS configuration commands
  redundancy            Display redundancy group parameters
  role                  Configure role parameters
  rtls                  Real Time Locating System commands
  running-config        Current Operating configuration
  securitymgr           Securitymgr parameters
  service-list          List of services
  sessions              Display current active open connections
  smtp-notification      Display SNMP engine parameters
  snmp                  Display SNMP engine parameters
  snmp-server           Display SNMP engine parameters
  spanning-tree         Display spanning tree information
  startup-config        Contents of startup configuration
  static-channel-group  Static channel group membership
  terminal              Display terminal configuration parameters
  timezone              Display timezone
  traffic-shape         Display traffic shaping
  upgrade-status        Display last image upgrade status
  users                 Display information about currently logged in users
  version               Display software & hardware version
  virtual-ip            IP redundancy feature
  wireless              Wireless configuration commands
  wlan-acl              wlan based acl
  wwan                  Wireless wan interfaces
RFController(config-crypto-isakmp)#show
```

Chapter

7

Crypto-group Instance

In this chapter

The `(config-crypto-group)` instance configures the default group properties of the ISAKMP client.

To navigate to this instance, use the command:

```
RFController(config)#crypto isakmp client configuration group default
RFController(config-crypto-group)#
```

Crypto Group config commands

Table 7 summarizes the controller **`config-crypto-group`** commands

TABLE 7 Crypto-group Instance Commands

Command	Description	Ref.
clrscr	Clears the display screen	*page 342*
dns	Defines a primary and secondary *Domain Name Server* (DNS)	*page 343*
end	Ends the current mode and moves to the EXEC mode	*page 344*
exit	Ends the current mode and moves to the previous mode	*page 345*
help	Displays the interactive help system	*page 346*
service	Invokes service commands to troubleshoot or debug the `(config-crypto-isakmp)` instance configuration	*page 347*
show	Shows running system information	*page 348*
wins	Defines a *Windows Name Server* (WINS)	*page 350*

clrscr

Crypto Group config commands

Clears the display screen

Supported in the following platforms:

- Mobility RFS4000 Controller
- Mobility RFS6000 Controller
- Mobility RFS7000 Controller

Syntax

```
clrscr
```

Parameters

None

Example

```
RFController(config-crypto-group)#clr
RFController(config-crypto-group)#
```

dns

Crypto Group config commands

Specifies the DNS server address(es) to assign to a client

Supported in the following platforms:

- Mobility RFS4000 Controller
- Mobility RFS6000 Controller
- Mobility RFS7000 Controller

Syntax

```
dns <IP>
```

<IP >	The first DNS server address to assign

Example

```
RFController(config-crypto-group)#dns-server 172.1.17.1
RFController(config-crypto-group)#
```

end

Crypto Group config commands

Ends and exits the current mode and changes to the PRIV EXEC mode. The prompt changes to `RFController#`

Supported in the following platforms:

- Mobility RFS4000 Controller
- Mobility RFS6000 Controller
- Mobility RFS7000 Controller

Syntax

```
end
```

Parameters

None

Example

```
RFController(config-crypto-group)#end
RFController#
```

exit

Crypto Group config commands

Ends the current mode and moves to the previous mode (GLOBAL-CONFIG). The prompt changes to `RFController(config)#`

Supported in the following platforms:

- Mobility RFS4000 Controller
- Mobility RFS6000 Controller
- Mobility RFS7000 Controller

Syntax

```
exit
```

Parameters

None

Example

```
RFController(config-crypto-group)#exit
RFController(config)#
```

help

Crypto Group config commands

Displays the system's interactive help system

Supported in the following platforms:

- Mobility RFS4000 Controller
- Mobility RFS6000 Controller
- Mobility RFS7000 Controller

Syntax

```
help
```

Parameters

None

Example

```
RFController(config-crypto-group)#help
CLI provides advanced help feature.  When you need help,
anytime at the command line please press '?'.

If nothing matches, the help list will be empty and you must backup
until entering a '?' shows the available options.
Two styles of help are provided:
1. Full help is available when you are ready to enter a
   command argument (e.g. 'show ?') and describes each possible
   argument.
2. Partial help is provided when an abbreviated argument is entered
   and you want to know what arguments match the input
   (e.g. 'show ve?'.)

RFController(config-crypto-group)#
```

service

Crypto Group config commands

Invokes service commands used troubleshoot or debug `(config-crypto-isakmp)` instance configurations

Supported in the following platforms:

- Mobility RFS4000 Controller
- Mobility RFS6000 Controller
- Mobility RFS7000 Controller

Syntax

```
service show cli
```

Parameters

cli	Displays the CLI tree of current mode

Example

```
RFController(config-crypto-group)#service show cli
Crypto Client Config mode:
+-clrscr [clrscr]
+-dns
  +-A.B.C.D [dns A.B.C.D]
+-do
  +-LINE [do LINE]
+-end [end]
+-exit [exit]
+-help [help]
+-quit [quit]
+-s
  +-commands [show commands]
    +-WORD [show commands WORD]
  +-running-config [show running-config]
    +-full [show running-config full]
    +-include-factory [show running-config include-factory]

.............................................
.............................................
RFController(config-crypto-group)#
```

show

Crypto Group config commands

Displays current system information running on the controller

Supported in the following platforms:

- Mobility RFS4000 Controller
- Mobility RFS6000 Controller
- Mobility RFS7000 Controller

NOTE
The following commands display only for the Mobility RFS6000 Controller and the Mobility RFS4000 Controller:
- power
The following commands display only for the Mobility RFS7000 Controller and the Mobility RFS4000 Controller:
- port-channel
- static-channel-group

NOTE
For more details on the show command see *show on page 59*

Syntax

```
show <paramater>
```

Parameters

?	Displays all the parameters for which information can be viewed using the show command

Example

```
RFController(config-crypto-group)#show ?
  access-list           Internet Protocol (IP)
  aclstats              Show ACL Statistics information
  alarm-log             Display all alarms currently in the system
  autoinstall           autoinstall configuration
  banner                Display Message of the Day Login banner
  boot                  Display boot configuration.
  clock                 Display system clock
  commands              Show command lists
  crypto                encryption module
  debugging             Debugging information outputs
  dhcp                  DHCP Server Configuration
  environment           show environmental information
  file                  Display filesystem information
  firewall              Wireless firewall
  ftp                   Display FTP Server configuration
  history               Display the session command history
  interfaces            Interface status
  ip                    Internet Protocol (IP)
  ldap                  LDAP server
  licenses              Show any installed licenses
  logging               Show logging configuration and buffer
```

```
  mac                   Internet Protocol (IP)
  mac-address-table     Display MAC address table
  mac-name              Displays the configured MAC Names
  management            Display L3 Managment Interface name
  mobility              Display Mobility parameters
  ntp                   Network time protocol
  password-encryption   password encryption
  port-channel          Portchannel commands
  port                  Physical/Aggregate port interface
  privilege             Show current privilege level
  protocol-list         List of protocols
  radius                RADIUS configuration commands
  redundancy            Display redundancy group parameters
  role                  Configures role parameters
  rtls                  Real Time Locating System commands
  running-config        Current Operating configuration
  securitymgr           Securitymgr parameters
  sessions              Display current active open connections
  smtp-notification     Display SNMP engine parameters
  snmp                  Display SNMP engine parameters
  snmp-server           Display SNMP engine parameters
  spanning-tree         Display spanning tree information
  startup-config        Contents of startup configuration
  static-channel-group  static channel group membership
  terminal              Display terminal configuration parameters
  timezone              Display timezone
  traffic-shape         Display traffic shaping
  upgrade-status        Display last image upgrade status
  users                 Display information about currently logged in users
  version               Display software & hardware version
  virtual-ip            IP redundancy feature
  wireless              Wireless configuration commands
  wlan-acl              wlan based acl
  wwan                  Wireless wan interfaces

RFController(config-crypto-group)#show
```

wins

Crypto Group config commands

Specifies the *Windows Internet Naming Service* (WINS) servers to assign to a client

Supported in the following platforms:

- Mobility RFS4000 Controller
- Mobility RFS6000 Controller
- Mobility RFS7000 Controller

Syntax

```
wins <IP>
```

Parameters

<IP >	The first WINS server address to assign

Example

```
RFController(config-crypto-group)#wins 128.2.11.1
RFController(config-crypto-group)#
```

Chapter

8

Crypto-peer Instance

In this chapter

The `(config-crypto-peer)` instance to configure ISAKMP peers. To enter this instance, use the command:

```
RFController(config)#crypto isakmp peer [address|dn|hostname]
RFController(config-crypto-peer)#
```

Crypto Peer config commands

Table 8 summarizes the **`config-crypto-peer`** commands

TABLE 8 Crypto Peer Command Summary

Command	*Description*	*Ref.*
clrscr	Clears the display screen	*page 352*
end	Ends the current mode and moves to the EXEC mode	*page 353*
exit	Ends the current mode and moves to the previous mode	*page 354*
help	Displays the system's interactive help system	*page 355*
no	Negates a command or sets its defaults	*page 356*
service	Invokes service commands to troubleshoot or debug the `(config-crypto-peer)` instance configuration	*page 357*
set	Sets configuration parameters	*page 358*
show	Displays running system	*page 359*

clrscr

Crypto Peer config commands

Clears the display screen

Supported in the following platforms:

- Mobility RFS4000 Controller
- Mobility RFS6000 Controller
- Mobility RFS7000 Controller

Syntax

```
clrscr
```

Parameters

None

Example

```
RFController(config-crypto-peer)#clrscr
RFController(config-crypto-peer)
```

end

Crypto Peer config commands

Ends and exits the current mode and moves to the PRIV EXEC mode. The prompt changes to `RFController#`

Supported in the following platforms:

- Mobility RFS4000 Controller
- Mobility RFS6000 Controller
- Mobility RFS7000 Controller

Syntax

```
end
```

Parameters

None

Example

```
RFController(config-crypto-peer)#end
RFController#
```

exit

Crypto Peer config commands

Ends the current mode and moves to the previous mode (GLOBAL-CONFIG). The prompt changes to `RFController(config)#`

Supported in the following platforms:

- Mobility RFS4000 Controller
- Mobility RFS6000 Controller
- Mobility RFS7000 Controller

Syntax

```
exit
```

Parameters

None

Example

```
RFController(config-crypto-peer)#exit
RFController(config)#
```

help

Crypto Peer config commands

Accesses the system's interactive help system

Supported in the following platforms:

- Mobility RFS4000 Controller
- Mobility RFS6000 Controller
- Mobility RFS7000 Controller

Syntax

```
help
```

Parameters

None

Example

```
RFController(config-crypto-peer)#help
CLI provides advanced help feature.  When you need help,
anytime at the command line please press '?'.
If nothing matches, the help list will be empty and you must backup
until entering a '?' shows the available options.
Two styles of help are provided:
1. Full help is available when you are ready to enter a
   command argument (e.g. 'show ?') and describes each possible
   argument.
2. Partial help is provided when an abbreviated argument is entered
   and you want to know what arguments match the input
   (e.g. 'show ve?'.)
RFController(config-crypto-peer)#
```

no

Crypto Peer config commands

Negates a command or sets it's defaults

Supported in the following platforms:

- Mobility RFS4000 Controller
- Mobility RFS6000 Controller
- Mobility RFS7000 Controller

Syntax

```
no set aggressive-mode password
```

Parameters

See *set* command for parameters details

Example

```
RFController(config-crypto-peer)#no set aggrerssive-mode password
RFController(config-crypto-peer)#
```

service

Crypto Peer config commands

Invokes service commands to troubleshoot or debug the `(config-crypto-peer)` instance configuration.

Supported in the following platforms:

- Mobility RFS4000 Controller
- Mobility RFS6000 Controller
- Mobility RFS7000 Controller

Syntax

```
service show cli
```

Parameters

cli	Displays the CLI tree of current mode

Example

```
RFController(config-crypto-peer)#service show cli
Crypto Peer Config mode:
+-clrscr [clrscr]
+-do
  +-LINE [do LINE]
+-end [end]
+-exit [exit]
+-help [help]
+-no
  +-set
    +-aggressive-mode
      +-password [no set aggressive-mode password]
+-quit [quit]
+-s
  +-commands [show commands]
    +-WORD [show commands WORD]
  +-running-config [show running-config]
    +-full [show running-config full]
    +-include-factory [show running-config include-factory]
.................................
.................................

RFController(config-crypto-peer)#
```

set

Crypto Peer config commands

Configures the aggressive-mode of `config-crypto-peer`

Supported in the following platforms:

- Mobility RFS4000 Controller
- Mobility RFS6000 Controller
- Mobility RFS7000 Controller

Syntax

```
set aggressive-mode password [0 <password>|2 <password>|
<password>]
```

Parameters

aggressive-mode password [0 <password>|2 <password>|<password>	Defines aggressive mode attributes
	• password – Specifies a tunnel-password attribute
	  • 0 <password> – Password <password> is specified unencrypted.
	  • 2 <password> – Password <password> is specified encrypted with the password-encryption secret
	  • <password> – The password of minimum size of 8 characters.

Example

```
RFController(config-crypto-peer)#set aggressive-mode password CheckMeIn
RFController(config-crypto-peer)#
```

show

Crypto Peer config commands

Displays current system information running on the controller

Supported in the following platforms:

Supported in the following platforms:

- Mobility RFS4000 Controller
- Mobility RFS6000 Controller
- Mobility RFS7000 Controller

NOTE
The following commands display only for the Mobility RFS6000 Controller and the Mobility RFS4000 Controller:
- power
The following commands display only for the Mobility RFS7000 Controller and the Mobility RFS4000 Controller:
- port-channel
- static-channel-group

NOTE
For more details on the show command see *show on page 59*

Syntax

```
show <paramater>
```

Parameters

?	Displays all the parameters for which information can be viewed using the show command.

Example

```
RFController(config-crypto-peer)#show ?
access-list           Internet Protocol (IP)
  aclstats              Show ACL Statistics information
  alarm-log             Display all alarms currently in the system
  autoinstall           autoinstall configuration
  banner                Display Message of the Day Login banner
  boot                  Display boot configuration.
  clock                 Display system clock
  commands              Show command lists
  crypto                encryption module
  debugging             Debugging information outputs
  dhcp                  DHCP Server Configuration
  environment           show environmental information
  file                  Display filesystem information
  firewall              Wireless firewall
  ftp                   Display FTP Server configuration
  history               Display the session command history
  interfaces            Interface status
  ip                    Internet Protocol (IP)
  ldap                  LDAP server
  licenses              Show any installed licenses
```

```
  logging               Show logging configuration and buffer
  mac                   Internet Protocol (IP)
  mac-address-table     Display MAC address table
  mac-name              Displays the configured MAC names
  management            Display L3 Managment Interface name
  mobility              Display Mobility parameters
  ntp                   Network time protocol
  password-encryption   password encryption
  port                  Physical/Aggregate port interface
  port-channel          Portchannel commands
  privilege             Show current privilege level
  protocol-list         List of protocols
  radius                RADIUS configuration commands
  role                  Configure role parameters
  redundancy            Display redundancy group parameters
  rtls                  Real Time Locating System commands
  running-config        Current Operating configuration
  securitymgr           Securitymgr parameters
  service-list          Displays list of services
  smtp-notifications    Display SNMP engine parameters
  sessions              Display current active open connections
  snmp                  Display SNMP engine parameters
  snmp-server           Display SNMP engine parameters
  spanning-tree         Display spanning tree information
  startup-config        Contents of startup configuration
  static-channel-group  static channel group membership
  terminal              Display terminal configuration parameters
  timezone              Display timezone
  upgrade-status        Display last image upgrade status
  users                 Display information about currently logged in users
  version               Display software & hardware version
  virtual-ip            IP redundancy feature
  wireless              Wireless configuration commands
  wlan-acl              wlan based acl
  wwan                  Wireless wan interfaces

RFController(config-crypto-peer)#show
```

Chapter

Crypto-ipsec Instance

9

In this chapter

Use the `(config-crypto-ipsec)` instance to define the transform configuration for securing data (esp-3des, esp-sha-hmac etc.).

To navigate to this instance, use the command

```
RFController(config)#crypto ipsec transform-set
       <transform-set-name> <encryption-type> <auth-type>
RFController(config-crypto-ipsec)#
```

The transform set is assigned to a crypto map using the map's transform-set command. For more details, see "set" on page 380.

Crypto IPSec config commands

The table below summarizes the **`config-crypto-ipsec`** commands:

TABLE 9 Crypto IPsec Command Summary

Command	Description	Ref.
show	Displays running system information	*page 367*
mode	Configures the IP Sec transportation mode	*page 365*
show	Clears the display screen	*page 59*
end	Ends the current mode and moves to the EXEC mode	*page 362*
exit	Ends the current mode and moves to the previous mode	*page 363*
help	Describes the interactive help system	*page 364*
no	Negates a command or set its defaults	*page 366*
service	Invokes service commands to troubleshoot or debug **`(config-crypto-isakmp)`** instance configurations	*page 369*

end

Crypto IPSec config commands

Ends and exits the current mode and moves to the PRIV EXEC mode. The prompt changes to `RFController#`

Supported in the following platforms:

- Mobility RFS4000 Controller
- Mobility RFS6000 Controller
- Mobility RFS7000 Controller

Syntax

```
end
```

Parameters

None

Example

```
RFController(config-crypto-ipsec)#end
RFController#
```

exit

Crypto IPSec config commands

Ends the current mode and moves to the previous mode (GLOBAL-CONFIG). The prompt changes to `RFController(config)#`

Supported in the following platforms:

- Mobility RFS4000 Controller
- Mobility RFS6000 Controller
- Mobility RFS7000 Controller

Syntax

```
exit
```

Parameters

None

Example

```
RFController(config-crypto-ipsec)#exit
RFController(config)#
```

help

Crypto IPSec config commands

Accesses the system's interactive help system

Supported in the following platforms:

- Mobility RFS4000 Controller
- Mobility RFS6000 Controller
- Mobility RFS7000 Controller

Syntax

```
help
```

Parameters

None

Example

```
RFController(config-crypto-peer)#help
CLI provides advanced help feature.  When you need help,
anytime at the command line please press '?'.
If nothing matches, the help list will be empty and you must backup
until entering a '?' shows the available options.
Two styles of help are provided:
1. Full help is available when you are ready to enter a
   command argument (e.g. 'show ?') and describes each possible
   argument.
2. Partial help is provided when an abbreviated argument is entered
   and you want to know what arguments match the input
   (e.g. 'show ve?'.)
RFController(config-crypto-peer)#
```

mode

Crypto IPSec config commands

Configures the IPSec mode of operation

Supported in the following platforms:

- Mobility RFS4000 Controller
- Mobility RFS6000 Controller
- Mobility RFS7000 Controller

Syntax

```
mode [transport|tunnel]
```

Parameters

transport	Transport mode
tunnel	Tunnel mode

Example

```
RFController(config-crypto-ipsec)#mode transport
RFController(config-crypto-ipsec)#
```

no

Crypto IPSec config commands

Negates a command or sets it's defaults

Supported in the following platforms:

- Mobility RFS4000 Controller
- Mobility RFS6000 Controller
- Mobility RFS7000 Controller

Syntax

```
no mode
```

Parameters

mode	Sets default to tunnel mode.

Example

```
RFController(config-crypto-ipsec)#no mode
RFController(config-crypto-ipsec)#
```

show

Crypto IPSec config commands

Use this command to view current system information running on the controller

Supported in the following platforms:

- Mobility RFS4000 Controller
- Mobility RFS6000 Controller
- Mobility RFS7000 Controller

NOTE
The following commands display only for the Mobility RFS6000 Controller and the Mobility RFS4000 Controller:
- power
The following commands display only for the Mobility RFS7000 Controller and the Mobility RFS4000 Controller:
- port-channel
- static-channel-group

Syntax

```
show <paramater>
```

Parameters

?	Displays all the parameters for which information can be viewed using the show command

Example

```
RFController(config-crypto-ipsec)#show ?
aclstats               Show ACL Statistics information
  alarm-log              Display all alarms currently in the system
  autoinstall            autoinstall configuration
  banner                 Display Message of the Day Login banner
  boot                   Display boot configuration.
  clock                  Display system clock
  commands               Show command lists
  crypto                 encryption module
  debugging              Debugging information outputs
  dhcp                   DHCP Server Configuration
  environment            show environmental information
  file                   Display filesystem information
  firewall               Wireless firewall
  ftp                    Display FTP Server configuration
  history                Display the session command history
  interfaces             Interface status
  ip                     Internet Protocol (IP)
  ldap                   LDAP server
  licenses               Show any installed licenses
  logging                Show logging configuration and buffer
  mac                    Internet Protocol (IP)
  mac-address-table      Display MAC address table
  mac-name               Displays the configured MAC names
  management             Display L3 Managment Interface name
  mobility               Display Mobility parameters
```

```
ntp                   Network time protocol
password-encryption   password encryption
port                  Physical/Aggregate port interface
port-channel          Portchannel commands
privilege             Show current privilege level
protocol-list         List of protocols
radius                RADIUS configuration commands
role                  Configure role parameters
redundancy            Display redundancy group parameters
rtls                  Real Time Locating System commands
running-config        Current Operating configuration
securitymgr           Securitymgr parameters
service-list          Displays list of services
smtp-notifications    Display SNMP engine parameters
sessions              Display current active open connections
snmp                  Display SNMP engine parameters
snmp-server           Display SNMP engine parameters
spanning-tree         Display spanning tree information
startup-config        Contents of startup configuration
static-channel-group  static channel group membership
terminal              Display terminal configuration parameters
timezone              Display timezone
upgrade-status        Display last image upgrade status
users                 Display information about currently logged in users
version               Display software & hardware version
virtual-ip            IP redundancy feature
wireless              Wireless configuration commands
wlan-acl              wlan based acl
wwan                  Wireless wan interfaces
```

RFController(config-crypto-ipsec)#show

service

Crypto IPSec config commands

Invokes service commands to troubleshoot or debug the `(config-crypto-peer)` instance configuration

Supported in the following platforms:

- Mobility RFS4000 Controller
- Mobility RFS6000 Controller
- Mobility RFS7000 Controller

Syntax

```
service show cli
```

Parameters

cli	Displays the CLI tree of current mode

Example

```
RFController(config-crypto-ipsec)#service show cli
Crypto Ipsec Config mode:
+-help [help]
+-show
  +-commands [show commands]
    +-WORD [show commands WORD]
  +-ip
    +-http
      +-secure-server [show ip http secure-server]
      +-server [show ip http server]
    +-access-group
      +-WORD [show ip access-group `WORD|ge <1-4>|me1|sa <1-4>|vlan <1-4094>']
      +-ge
        +-<1-4> [show ip access-group `WORD|ge <1-4>|me1|sa <1-4>|vlan
<1-4094>']
      +-me1 [show ip access-group `WORD|ge <1-4>|me1|sa <1-4>|vlan <1-4094>']
.................................
.................................

RFController(config-crypto-peer)#
```

Chapter

Crypto-map Instance

10

In this chapter

The `(config-crypto-map)` commands define a *Certificate Authority* (CA) trustpoint. This is a separate instance, but belongs to the `crypto pki trustpoint` mode under the `config` instance.

To navigate to this instance, use the command:

```
RFController(config)#crypto map <map-name> <sequence>
       [ipsec-isakmp|ipsec-manual] {dynamic}
RFController(config-crypto-map)#
```

Crypto Map config commands

Table 10 summarizes `config-crypto-map` commands:

TABLE 10 Crypto Map Command Summary

Command	Description	Ref.
clrscr	Clears the display screen	*page 372*
end	Ends the current mode and moves to the EXEC mode	*page 373*
exit	Ends the current mode and moves to the previous mode	*page 374*
help	Describes the interactive help system	*page 375*
match	Assigns an IP access-list to a crypto map definition	*page 376*
no	Negates a command or set its defaults	*page 378*
service	Invokes service commands to troubleshoot or debug the instance configurations	*page 379*
set	Sets values for encryption/decryption parameters	*page 380*
show	Displays the running system information	*page 384*

clrscr

Crypto Map config commands

Clears the display screen

Supported in the following platforms:

- Mobility RFS4000 Controller
- Mobility RFS6000 Controller
- Mobility RFS7000 Controller

Syntax

```
clrscr
```

Parameters

None

Example

```
RFController(config-crypto-map)#clrscr
RFController(config-crypto-map)#
```

end

Crypto Map config commands

Ends and exits the current mode and moves to the to PRIV EXEC mode. The prompt changes to `RFController#`

Supported in the following platforms:

- Mobility RFS4000 Controller
- Mobility RFS6000 Controller
- Mobility RFS7000 Controller

Syntax

```
end
```

Parameters

None

Example

```
RFController(config-crypto-map)#end
RFController#
```

exit

Crypto Map config commands

Ends the current mode and moves to the previous mode (GLOBAL-CONFIG). The prompt changes to `RFController(config)#`

Supported in the following platforms:

- Mobility RFS4000 Controller
- Mobility RFS6000 Controller
- Mobility RFS7000 Controller

Syntax

```
exit
```

Parameters

None

Example

```
RFController(config-crypto-map)#exit
RFController(config)#
```

help

Crypto Map config commands

Displays the system's interactive help system

Supported in the following platforms:

- Mobility RFS4000 Controller
- Mobility RFS6000 Controller
- Mobility RFS7000 Controller

Syntax

```
help
```

Parameters

None

Example

```
RFController(config-crypto-map)#help
CLI provides advanced help feature.  When you need help,
anytime at the command line please press '?'.

If nothing matches, the help list will be empty and you must backup
until entering a '?' shows the available options.
Two styles of help are provided:
1. Full help is available when you are ready to enter a
   command argument (e.g. 'show ?') and describes each possible
   argument.
2. Partial help is provided when an abbreviated argument is entered
   and you want to know what arguments match the input
   (e.g. 'show ve?'.)
RFController(config-crypto-map)#
```

match

Crypto Map config commands

Use this command to assign an IP access-list to a crypto map definition. The access-list designates the IP packets to be encrypted by this crypto map.

A crypto map entry is a single policy that describes how certain traffic is secured. There are two types of crypto map entries: ipsec-manual and ipsec-ike entries. Each entry is given an index (used to sort the ordered list).

When a non-secured packet arrives on an interface, the crypto map set associated with that interface is processed (in order). If a crypto map entry matches the non-secured traffic, the traffic is discarded.

When a packet is transmitted on an interface, the crypto map set associated with that interface is processed. The first crypto map entry that matches the packet is used to secure the packet. If a suitable SA exists, it is used for transmission. Otherwise, IKE is used to establish an SA with the peer. If no SA exists (and the crypto map entry is “respond only”), the packet is discarded.

When a secured packet arrives on an interface, its SPI is used to look up a SA. If a SA does not exist (or if the packet fails any of the security checks), it is discarded. If all checks pass, the packet is forwarded normally.

Supported in the following platforms:

- Mobility RFS4000 Controller
- Mobility RFS6000 Controller
- Mobility RFS7000 Controller

Syntax

```
match address <acl-id>
```

Parameters

address	Match the address of packets to encrypt
<acl-id>	Enter the name of the access list or ACL ID to assign to this crypto map

Usage Guidelines

Crypto map entries do not directly contain the selectors used to determine which data to secure. Instead, the crypto map entry refers to an access control list. An access control list (ACL) is assigned to the crypto map using the match address command. If no ACL is configured for a crypto map, the entry is incomplete and will have no effect on the system.

The entries of the ACL used in a crypto map should be created with respect to traffic sent by the OS. The source information must be the local OS, and the destination must be the peer.

Only extended access-lists can be used in crypto maps.

Example

The following entails setting up an ACL (called TestList) and assigning the new list to a crypto map (called TestMap):

```
RFController(config)#ip access-list extended TestList
Configuring New Extended ACL "TestList"
```

```
(config-ext-nacl)#exit

RFController(config)#crypto map TestMap 220 isakmp dynamic
RFController(config-crypto-map)#

RFController(config-crypto-map)#match address TestMap
RFController(config-crypto-map)#
```

no

Crypto Map config commands

Negates a command or sets its defaults

Supported in the following platforms:

- Mobility RFS4000 Controller
- Mobility RFS6000 Controller
- Mobility RFS7000 Controller

Syntax

```
no [match|set]
```

Parameters

Use the commands configured under this instance.

Example

```
RFController(config-crypto-map)#no match address <WORD>
RFController(config-crypto-map)#
```

service

Crypto Map config commands

Invokes service commands to troubleshoot or debug the `(config-crypto-peer)` instance configuration

Supported in the following platforms:

- Mobility RFS4000 Controller
- Mobility RFS6000 Controller
- Mobility RFS7000 Controller

Syntax

```
service show cli
```

Parameters

cli	Displays the CLI tree of the current mode

Example

```
RFController(config-crypto-map)#service show cli
Crypto Map Config mode:
+-clrscr [clrscr]
+-do
  +-LINE [do LINE]
+-end [end]
+-exit [exit]
+-help [help]
+-match
  +-address
    +-WORD [match address WORD]
+-no
  +-match
    +-address
      +-WORD [no match address WORD]
  +-set
    +-localid [no set localid]
    +-mode [no set mode]
    +-peer
      +-A.B.C.D [no set peer (A.B.C.D |WORD)]
      +-WORD [no set peer (A.B.C.D |WORD)]
    +-pfs [no set pfs]
    +-remote-type [no set remote-type]
    +-security-association
      +-level
        +-perhost [no set security-association level perhost]
      +-lifetime [no set security-association lifetime]
    +-session-key
      +-inbound
        +-ah [no set session-key ( inbound | outbound ) ah]
        +-esp [no set session-key ( inbound | outbound ) esp]
.....................................................................
.....................................................................
.........................................
RFController(config-crypto-map)#
```

set

Crypto Map config commands

Configures set parameters for the peer device

Supported in the following platforms:

- Mobility RFS4000 Controller
- Mobility RFS6000 Controller
- Mobility RFS7000 Controller

Syntax

```
set [localid|mode|peer|pfs|remote-type {ipsec-l2tp|xauth}|
security-association|session-key|transform-set)

set localid [dn|hostname]<name>

set pfs [1|2|5]

set mode [aggressive|main]

set security-association [level|lifetime]
set security-association level perhost
set security-association lifetime [kilobytes|seconds]<value>

set session-key [inbound|outbound]{ah|esp}
set session-key [inbound|outbound] ah <hexkey data>
set session-key [inbound|outbound] esp <SPI>cipher<hexdata key> authenticator
<hexkey data>
set peer [ipaddress|<host name>]

set remote-type [ipsec-l2tp|xauth]
set transform-set <name>
```

Parameters

localid [dn|hostname] <name>	Sets the local identity • dn <name> – Defines the distinguished dn name • hostname <name> – Sets the hostname • <name> – The distinguished name or hostname
mode [aggressive|main]	Sets the mode of the tunnels for this Crypto Map • aggressive – Initiates aggressive mode • main – Initiates main mode
peer [ipaddress| <host name>]	Sets the IP address of the peer device. This can be set for multiple remote peers. The remote peer can be either an IP address. In manual mode, only one remote peer can be added for a crypto map • IP address – Enter the IP address of the peer device. If not configured, it implies responder only to any peer • <host name> – Displays host name of the peer
pfs [1|2|5]	Use the *set pfs* command to choose the type of perfect forward secrecy (if any) required during IPSec negotiation of SAs for this crypto map. Use the no form of this command to require no PFS. • group 1 – IPSec is required to use the Diffie-Hellman Group 1 (768-bit modulus) exchange during IPSec SA key generation • group 2 – IPSec is required to use the Diffie-Hellman Group 2 (1024-bit modulus) exchange during IPSec SA key generation • group 5 – IPSec is required to use Diffie-Hellman Group 5
remote-type [ipsec-l2tp| xauth]	Sets the remote VPN client type • ipsec-l2tp – Specify the remote VPN client as using IPSEC/L2TP • xauth – Specify the remote VPN client as using XAUTH with mode config
security-association [level perhost|lifetime {kilobyte|seconds}]	Defines the lifetime (in kilobytes and/or seconds) of the IPSec SAs created by this crypto map • level perhost – Specifies the security association granularity level for identities • lifetime [kilobyte|seconds] – Security an association lifetime

session-key [inbound|outbound] {ah|esp} <256-4294967295> cipher	Use the set session-key command to define the encryption and authentication keys for this crypto map
	• inbound [ah|esp] – Defines encryption keys for inbound traffic
	• outbound [ah|esp] – Defines encryption keys for outbound traffic
	For information on how to create a key for authentication and encryption, refer Usage Guideline in *Global Configuration commands* under *crypto on page 233*.
	• ah <256-4294967295> – Authentication header protocol
	  • <256-4294967295> – *Security Parameter Index* (SPI) for the security association
	• esp <256-4294967295>– Encapsulating security payload protocol
	  • <256-4294967295> cipher – Defines the security parameter index
	  • cipher – Specify encryption/decryption key
	authenticator <hex key data> – Specify an authentication key

transformset <name>	Use the set transform-set command to assign a transform-set to a crypto map

Usage Guidelines

```
RFController(config-crypto-map)#set peer name
```

If no peer IP address is configured, the manual crypto map is not valid and not complete. A peer IP address is required for manual crypto maps. To change the peer IP address, the no set peer command must be issued first; then the new peer IP address can be configured.

```
RFController(config-crypto-map)#set pfs
```

If left at the default setting, no *perfect forward secrecy* (PFS) is used during IPSec SA key generation. If PFS is specified, the specified Diffie-Hellman Group exchange is used for the initial (and all subsequent) key generations. This means no data linkage between prior keys and future keys.

```
RFController(config-crypto-map)#set security-association lifetime
(kilobytes|seconds)
```

Values can be entered in both kilobytes and seconds. Whichever limit is reached first, ends the security association.

```
RFController(config-crypto-map)#set session-key [inbound|outbound]{ah|esp}

RFController(config-crypto-map)#set session-key [inbound|outbound] ah <hexkey
data>

RFController(config-crypto-map)#set session-key [inbound|outbound] esp <SPI>
cipher <hexdata key> authenticator <hexkey data>
```

The inbound local SPI (security parameter index) must equal the outbound remote SPI. The outbound local SPI must equal the inbound remote SPI. The key values are the hexadecimal representations of the keys.

They are not true ASCII strings. Therefore, a key of 3031323334353637 represents “01234567”.

```
RFController(config-crypto-map)#set transformset name
```

Crypto map entries do not directly contain the transform configuration for securing data. Instead, the crypto map is associated with transform sets which contain specific security algorithms.

If a transform-set is not configured for a crypto map, the entry is incomplete and has no effect. For manual key crypto maps, only one transform set can be specified.

Example

```
RFController(config-crypto-map)#set localid hostname TestMapHost
RFController(config-crypto-map)#
```

show

Crypto Map config commands

Displays current system information running on the controller

Supported in the following platforms:

- Mobility RFS4000 Controller
- Mobility RFS6000 Controller
- Mobility RFS7000 Controller

NOTE
The following commands display only for the Mobility RFS6000 Controller and the Mobility RFS4000 Controller:
- power
The following commands display only for the Mobility RFS7000 Controller and the Mobility RFS4000 Controller:
- port-channel
- static-channel-group

Syntax

```
show <paramater>
```

Parameters

?	Displays all the parameters for which information can be viewed using the show command

Example

```
RFController(config-crypto-map)#show ?
RFController(config-crypto-ipsec)#show ?
  aclstats              Show ACL Statistics information
  alarm-log             Display all alarms currently in the system
  autoinstall           autoinstall configuration
  banner                Display Message of the Day Login banner
  boot                  Display boot configuration.
  clock                 Display system clock
  commands              Show command lists
  crypto                encryption module
  debugging             Debugging information outputs
  dhcp                  DHCP Server Configuration
  environment           show environmental information
  file                  Display filesystem information
  firewall              Wireless firewall
  ftp                   Display FTP Server configuration
  history               Display the session command history
  interfaces            Interface status
  ip                    Internet Protocol (IP)
  ldap                  LDAP server
  licenses              Show any installed licenses
  logging               Show logging configuration and buffer
  mac                   Internet Protocol (IP)
  mac-address-table     Display MAC address table
  mac-name              Displays the configured MAC names
  management            Display L3 Managment Interface name
```

```
  mobility              Display Mobility parameters
  ntp                   Network time protocol
  password-encryption   password encryption
  port                  Physical/Aggregate port interface
  port-channel          Portchannel commands
  privilege             Show current privilege level
  protocol-list         List of protocols
  radius                RADIUS configuration commands
  role                  Configure role parameters
  redundancy            Display redundancy group parameters
  rtls                  Real Time Locating System commands
  running-config        Current Operating configuration
  securitymgr           Securitymgr parameters
  service-list          Displays list of services
  smtp-notifications    Display SNMP engine parameters
  sessions              Display current active open connections
  snmp                  Display SNMP engine parameters
  snmp-server           Display SNMP engine parameters
  spanning-tree         Display spanning tree information
  startup-config        Contents of startup configuration
  static-channel-group  static channel group membership
  terminal              Display terminal configuration parameters
  timezone              Display timezone
  upgrade-status        Display last image upgrade status
  users                 Display information about currently logged in users
  version               Display software & hardware version
  virtual-ip            IP redundancy feature
  wireless              Wireless configuration commands
  wlan-acl              wlan based acl
  wwan                  Wireless wan interfaces

RFController(config-crypto-map)#show
```

Chapter

Crypto-trustpoint Instance

11

In this chapter

The `(config-crypto-trustpoint)` commands define a Certificate Authority (CA) trustpoint. This is a separate instance, but belongs to the `crypto pki trustpoint` mode under the `config` instance.

To navigate to this instance, use the command

```
RFController(config)#crypto pki trustpoint <trustpoint-name>
RFController(config-trustpoint)#
```

Trustpoint (PKI) config commands

Table 11 summarizes `config-crypto-trustpoint` commands:

TABLE 11 Trustpoint (PKI) Config Command Summary

Command	Description	Ref.
clrscr	Clears the display screen	*page 388*
company-name	Defines a company name for the trustpoint	*page 389*
email	Sets an e-mail ID for the trustpoint	*page 390*
end	Ends the current mode and moves to the EXEC mode	*page 391*
exit	Ends the current mode and moves to the previous mode	*page 392*
fqdn	Sets the domain name of the trustpoint	*page 393*
help	Displays the interactive help system	*page 394*
ip-address	Sets an IP address for the trustpoint	*page 395*
no	Negates a command or sets its defaults	*page 396*
password	Sets the challenge password (applicable only for requests), to access the trustpoint	*page 397*
rsakeypair	Defines a RSA Keypair to associate with the trustpoint	*page 398*
service	Invokes service commands to troubleshoot or debug the `crypto pki trustpoint` instance configuration	*page 399*
show	Displays running system information	*page 400*
subject-name	The subject name is a collection of required parameters to configure a trustpoint	*page 402*

clrscr

Trustpoint (PKI) config commands

Clears the display screen

Supported in the following platforms:

- Mobility RFS4000 Controller
- Mobility RFS6000 Controller
- Mobility RFS7000 Controller

Syntax

```
clrscr
```

Parameters

None

Example

```
RFController(config-trustpoint)#clrscr
RFController(config-trustpoint)#
```

company-name

Trustpoint (PKI) config commands

Sets the company name (Applicable only for request)

Supported in the following platforms:

- Mobility RFS4000 Controller
- Mobility RFS6000 Controller
- Mobility RFS7000 Controller

Syntax

```
company-name <company-name>
```

Parameters

<company-name>	Company name (2 to 64 characters)

Example

```
RFController(config-trustpoint)#company-name RetailKing
RFController(config-trustpoint)#
```

email

Trustpoint (PKI) config commands

Sets the e-mail ID for the trustpoint

Supported in the following platforms:

- Mobility RFS4000 Controller
- Mobility RFS6000 Controller
- Mobility RFS7000 Controller

Syntax

```
email <email>
```

Parameters

<email>	Sets email address (2 to 64 characters) for the trustpoint

Example

```
RFController(config-trustpoint)#email abcTestemailID@brocade.com
RFController(config-trustpoint)#
```

end

Trustpoint (PKI) config commands

Ends and exits the current mode and moves to the PRIV EXEC mode. The prompt changes to `RFController#`

Supported in the following platforms:

- Mobility RFS4000 Controller
- Mobility RFS6000 Controller
- Mobility RFS7000 Controller

Syntax

```
end
```

Parameters

None

Example

```
RFController(config-trustpoint)#end
RFController#
```

exit

Trustpoint (PKI) config commands

Ends the current mode and moves to previous the mode (GLOBAL-CONFIG). The prompt changes to `RFController(config)#`

Supported in the following platforms:

- Mobility RFS4000 Controller
- Mobility RFS6000 Controller
- Mobility RFS7000 Controller

Syntax

```
exit
```

Parameters

None

Example

```
RFController(config-trustpoint)#exit
RFController(config)#
```

fqdn

Trustpoint (PKI) config commands

Configures the domain name of the trustpoint (FQDN stands for Fully Qualified Domain Name)

Supported in the following platforms:

- Mobility RFS4000 Controller
- Mobility RFS6000 Controller
- Mobility RFS7000 Controller

Syntax

```
fqdn <domain-name>
```

Parameters

<domain-name>	The fully qualified domain name (between 9 and 64 characters long)

Example

```
RFController(config-trustpoint)#fqdn RetailKing.com
RFController(config-trustpoint)#
```

help

Trustpoint (PKI) config commands

Displays the systems interactive help system

Supported in the following platforms:

- Mobility RFS4000 Controller
- Mobility RFS6000 Controller
- Mobility RFS7000 Controller

Syntax

```
help
```

Parameters

None

Example

```
RFController(config-trustpoint)#help
CLI provides advanced help feature. When you need help,
anytime at the command line please press '?'.

If nothing matches, the help list will be empty and you must backup
until entering a '?' shows the available options.
Two styles of help are provided:
1. Full help is available when you are ready to enter a
   command argument (e.g. 'show ?') and describes each possible
   argument.
2. Partial help is provided when an abbreviated argument is entered
   and you want to know what arguments match the input
   (e.g. 'show ve?'.)

RFController(config-trustpoint)#
```

ip-address

Trustpoint (PKI) config commands

Sets an IP address for the trustpoint

Supported in the following platforms:

- Mobility RFS4000 Controller
- Mobility RFS6000 Controller
- Mobility RFS7000 Controller

Syntax

```
ip-address <IP>
```

Parameters

<IP>	Enter the IP address for the trustpoint

Example

```
RFController(config-trustpoint)#ip-address 157.200.200.02
RFController(config-trustpoint)#
```

no

Trustpoint (PKI) config commands

Negates a command or sets its defaults

Supported in the following platforms:

- Mobility RFS4000 Controller
- Mobility RFS6000 Controller
- Mobility RFS7000 Controller

Syntax

```
no [company-name|email|fqdn|ip-address|subject-name]
```

Parameters

None.

Example

```
RFController(config-trustpoint)#no ip-address
RFController(config-trustpoint)#
```

password

Trustpoint (PKI) config commands

Sets the challenge password (applicable only for requests) to access the trustpoint

Supported in the following platforms:

- Mobility RFS4000 Controller
- Mobility RFS6000 Controller
- Mobility RFS7000 Controller

Syntax

```
password [0<password>|2<password>|<password>]
```

Parameters

0 <password>	Password <password> is specified as unencrypted, the password should be between 4 to 20 characters
2 <password>	Password <password> is encrypted with password-encryption secret, the string length of encrypted password should be between 44 - 64 characters
<password>	Sets the password to <password> (4 to 20 characters)

Example

```
RFController(config-trustpoint)#password 0 TestPassword
RFController(config-trustpoint)#
```

rsakeypair

Trustpoint (PKI) config commands

Configures a RSA Keypair to associate with the trustpoint

Supported in the following platforms:

- Mobility RFS4000 Controller
- Mobility RFS6000 Controller
- Mobility RFS7000 Controller

Syntax

```
rsakeypair <keypair-name>
```

Parameters

<keypair-name>	RSA Keypair Identifier

Usage Guidelines

The RSA key pair configures the controller to have *Rivest, Shamir, and Adelman* (RSA) key pairs. Thus, the controller software can maintain a different key pair for each identity certificate.

Example

```
RFController(config-trustpoint)#rsakeypair were
RFController(config-trustpoint)#
```

The rsakeypair name "*were*" in this example is an existing keypair value.

service

Trustpoint (PKI) config commands

Invokes service commands to troubleshoot or debug the `crypto pki trustpoint` instance configuration

Supported in the following platforms:

- Mobility RFS4000 Controller
- Mobility RFS6000 Controller
- Mobility RFS7000 Controller

Syntax

```
service show cli
```

Parameters

None

Example

```
RFController(config-trustpoint)#service show cli
Trustpoint Config mode:
+-clrscr [clrscr]
+-company-name
  +-WORD [company-name WORD]
+-do
  +-LINE [do LINE]
+-email
  +-WORD [email WORD]
+-end [end]
+-exit [exit]
+-fqdn
  +-WORD [fqdn WORD]
+-help [help]
+-ip-address
  +-A.B.C.D [ip-address A.B.C.D]
+-no
  +-company-name [no company-name]
  +-email [no email]
  +-fqdn [no fqdn]
  +-ip-address [no ip-address]
  +-subject-name [no subject-name]
.....................................................................
.....................................................................
.......................
RFController(config-trustpoint)#
```

show

Trustpoint (PKI) config commands

Displays current system information running on the controller

Supported in the following platforms:

- Mobility RFS4000 Controller
- Mobility RFS6000 Controller
- Mobility RFS7000 Controller

NOTE
The following commands display only for the Mobility RFS6000 Controller and the Mobility RFS4000 Controller:
- power
The following commands display only for the Mobility RFS7000 Controller and the Mobility RFS4000 Controller:
- port-channel
- static-channel-group

Syntax

```
show <paramater>
```

Parameters

?	Displays all the parameters for which information can be viewed using the show command

Example

```
RFController(config-trustpoint)#show ?
access-list           Internet Protocol (IP)
  aclstats              Show ACL Statistics information
  alarm-log             Display all alarms currently in the system
  autoinstall           autoinstall configuration
  banner                Display Message of the Day Login banner
  boot                  Display boot configuration.
  clock                 Display system clock
  commands              Show command lists
  crypto                encryption module
  debugging             Debugging information outputs
  dhcp                  DHCP Server Configuration
  environment           show environmental information
  file                  Display filesystem information
  firewall              Wireless firewall
  ftp                   Display FTP Server configuration
  history               Display the session command history
  interfaces            Interface status
  ip                    Internet Protocol (IP)
  ldap                  LDAP server
  licenses              Show any installed licenses
  logging               Show logging configuration and buffer
  mac                   Internet Protocol (IP)
  mac-address-table     Display MAC address table
  mac-name              Displays the configured MAC names
  management            Display L3 Managment Interface name
```

```
  mobility              Display Mobility parameters
  ntp                   Network time protocol
  password-encryption   password encryption
  port                  Physical/Aggregate port interface
  port-channel          Portchannel commands
  privilege             Show current privilege level
  protocol-list         List of protocols
  radius                RADIUS configuration commands
  redundancy            Display redundancy group parameters
  role                  Configure role parameters
  rtls                  Real Time Locating System commands
  running-config        Current Operating configuration
  securitymgr           Securitymgr parameters
  sessions              Display current active open connections
  smtp-notification     Display SNMP engine parameters
  snmp                  Display SNMP engine parameters
  snmp-server           Display SNMP engine parameters
  spanning-tree         Display spanning tree information
  startup-config        Contents of startup configuration
  static-channel-group  static channel group membership
  service-list          Displays list of services
  terminal              Display terminal configuration parameters
  traffic-shape         Display traffic shaping
  timezone              Display timezone
  upgrade-status        Display last image upgrade status
  users                 Display information about currently logged
                        in users
  version               Display software & hardware version
  virtual-ip            IP redundancy feature
  wireless              Wireless configuration commands
  wlan-acl              wlan based acl
  wwan                  Wireless wan interfaces

RFController(config-crypto-map)#show
```

subject-name

Trustpoint (PKI) config commands

Creates a subject name to configure a trustpoint (the subject name is a collection of required parameters to configure a trustpoint)

Supported in the following platforms:

- Mobility RFS4000 Controller
- Mobility RFS6000 Controller
- Mobility RFS7000 Controller

Syntax

```
subject-name <name> <country> <state> <city> <org>
<org-unit>
```

Parameters

<name>	Name of this set of parameters for configuring trust points
<country>	The 2 character ISO country code
<state>	The state in the country (2 to 128 characters)
<city>	The city name (2 to 128 characters)
<org>	The organization name (2 to 128 characters)
<org-unit>	The name of the unit in the organization (2 to 128 characters)

Example

```
RFController(config-trustpoint)#subject-name TestPool ?
  WORD  Country ( 2 character ISO Code )

RFController(config-trustpoint)#subject-name TestPool US ?
  WORD  State( 2 to 128 characters )

RFController(config-trustpoint)#subject-name TestPool US OH ?
  WORD  City( 2 to 128 characters )

RFController(config-trustpoint)#subject-name TestPool US OH PB ?
  WORD  Organization( 2 to 64 characters )

RFController(config-trustpoint)#subject-name TestPool US OH PB BROCADE ?
  WORD  Organization Unit( 2 to 64 characters )

RFController(config-trustpoint)#subject-name TestPool US OH PB BROCADE WID ?
  <cr>

RFController(config-trustpoint)#subject-name TestPool US OH PB BROCADE WID
RFController(config-trustpoint)#
```

Chapter

12

Interface Instance

In this chapter

Use the `(config-if)` instance to configure the interfaces – Ethernet, VLAN and tunnel associated with the controller.

To controller to this mode, use the command:

For Mobility RFS7000 Controller:

```
RFController(config)#interface [<interface-name>|ge <1-4>|me1|sa <1-4>|vlan
<1-4094>
RFController(config-if)#
```

For Mobility RFS6000 Controller:

```
RFController(config)#interface [<interface-name>|ge <1-8>|me1|up1|vlan
<1-4094>
RFController(config-if)#
```

For Mobility RFS4000 Controller:

```
RFSwitch(config)#interface [<interface-name>|ge <1-5>|me1|
    up1|vlan <1-4094>|sa <1-6>|wwan]
RFSwitch(config-if)#
```

Interface config commands

Table 12 summarizes the `(config-if)` commands:

TABLE 12 Interface Config Commands

Command	Description	Ref.
clrscr	Clears the display screen	*page 405*
crypto	Defines the encryption module	*page 406*
description	Creates an interface specific description	*page 407*
duplex	Sets the duplex mode used by the interface	*page 408*
end	Ends the current mode and moves to the EXEC mode	*page 409*
exit	Ends the current mode and moves to the previous mode	*page 410*
help	Displays the interactive help system	*page 411*
ip	Sets the IP address for the assigned ethernet, VLAN or tunnel	*page 412*
mac	Applies a MAC access list to a gigabit ethernet interface	*page 415*
management	Sets the selected interface as the management interface	*page 416*

TABLE 12 Interface Config Commands

Command	Description	Ref.
no	Negates a command or sets its defaults	*page 417*
port-channel	Configures the load-balancing criteria of an aggregated port	*page 418*
power	PoE (Power Over Ethernet) commands used to configure PoE power limit and priority for a port	*page 420*
service	Invokes service commands to troubleshoot or debug the **(config-if)** instance configurations	*page 421*
show	Displays running system information	*page 422*
shutdown	Shuts down a selected interface	*page 424*
spanning-tree	Disables the selected interface. The interface is administratively enabled unless explicitly disabled using this command	*page 425*
speed	Specifies the speed of a fast-ethernet (10/100) or a gigabit ethernet port (10/100/1000)	*page 428*
static-channel-group	Configures static channel commands	*page 429*
storm-control	Sets broadcast rate-limit value	*page 432*
controllerport	Sets controller mode characteristics	*page 430*
tunneling	Sets protocol-over protocol tunneling	*page 433*

clrscr

Interface config commands

Clears the display screen

Supported in the following platforms:

- Mobility RFS4000 Controller
- Mobility RFS6000 Controller
- Mobility RFS7000 Controller

Syntax

```
clrscr
```

Parameters

None

Example

```
RFController(config-if)#clrscr
RFController(config-if)#
```

crypto

Interface config commands

Sets the encryption module to use for this interface

Supported in the following platforms:

- Mobility RFS4000 Controller
- Mobility RFS6000 Controller
- Mobility RFS7000 Controller

Syntax

```
crypto map <map-tag>
```

Parameters

map <map-tag>	Assigns a Crypto Map • <map-tag> – Crypto Map tag

Usage Guidelines

At any given instance you can add one crypto mapset to an single interface. The controller does not allow the same cryptomap set to be attached to multiple interfaces.

description

Interface config commands

Creates an interface specific description

Supported in the following platforms:

- Mobility RFS4000 Controller
- Mobility RFS6000 Controller
- Mobility RFS7000 Controller

Syntax

```
description <description>
```

Parameters

<description>	Defines the characters describing this interface

Example

RFController(config-if)#description "interface for RetailKing"

```
RFController(config-if)#
```

duplex

Interface config commands

Specifies the duplex mode for the interface

NOTE
Duplexity can only be set for an Ethernet Interface. Enter the `(config-if)` instance using the `eth` parameter of the `interface` mode
The duplex cannot be set until the speed is set to a non-auto value

Supported in the following platforms:

- Mobility RFS4000 Controller
- Mobility RFS6000 Controller
- Mobility RFS7000 Controller

Syntax

```
duplex [auto|full|half]
```

Parameters

auto	Sets the ports duplexity automatically. The port automatically detects whether it should run in full or half-duplex mode
full	Sets the port in full-duplex mode
half	Sets the port in half-duplex mode

Usage Guidelines

The duplex defines the communication used by the port. The controller (by default) is set in the auto duplex mode. In auto mode, the duplex is selected based on connected network hardware.

end

Interface config commands

Ends and exits the current mode and moves to the PRIV EXEC mode. The prompt changes to `RFController#`

Supported in the following platforms:

- Mobility RFS4000 Controller
- Mobility RFS6000 Controller
- Mobility RFS7000 Controller

Syntax

```
end
```

Parameters

None

Example

```
RFController(config-if)#end
RFController#
```

exit

Interface config commands

Ends the current mode and moves to the previous mode (GLOBAL-CONFIG). The prompt changes to `RFController(config)#`

Supported in the following platforms:

- Mobility RFS4000 Controller
- Mobility RFS6000 Controller
- Mobility RFS7000 Controller

Syntax

```
exit
```

Parameters

None

Example

```
RFController(config-if)#exit
RFController(config)#
```

help

Interface config commands

Displays the system's interactive help

Supported in the following platforms:

- Mobility RFS4000 Controller
- Mobility RFS6000 Controller
- Mobility RFS7000 Controller

Syntax

```
help
```

Parameters

None

Example

```
RFController(config-if)#help
CLI provides advanced help feature.  When you need help,
anytime at the command line please press '?'.

If nothing matches, the help list will be empty and you must backup
until entering a '?' shows the available options.
Two styles of help are provided:
1. Full help is available when you are ready to enter a
   command argument (e.g. 'show ?') and describes each possible
   argument.
2. Partial help is provided when an abbreviated argument is entered
   and you want to know what arguments match the input
   (e.g. 'show ve?'.)

RFController(config-if)#
```

ip

Interface config commands

Sets the IP address for the assigned Fast Ethernet interface (ME) and VLAN Interface

Supported in the following platforms:

- Mobility RFS4000 Controller
- Mobility RFS6000 Controller
- Mobility RFS7000 Controller

Syntax

```
ip [access-group|address|arp|dhcp|helper-address|nat]
ip access-group [<1-99>|<100-199>|<1300-1999>|
<2000-2699>|WORD in]
ip arp [rate-limit|trust]
ip dhcp trust
ip address [<IP/Mask> {secondary}|dhcp]
ip helper-address <IP>
ip nat [inside|outside]
```

Parameters

access-group [<1-99>| <100-199>| <1300-1999>| <2000-2699>]	Defines the access group • <1-99> – Sets the IP standard access list • <100-199> – Sets the IP extended access list • <1300-1999> – Sets the IP standard access list (expanded range) • <2000-2699> – Sets the IP extended access list (expanded range) • WORD in – Defines the access list name • in – Sets incoming packets
ip address [<IP Mask> {secondary}|dhcp]	Sets a static IP address and network mask for a Layer 3 SVI (*Controller Virtual Interface*) • <IP/ Mask> {secondary} – Sets the IP address (10.0.0.1/8) • secondary – Defines an optional secondary IP address • dhcp – Uses a DHCP Client to obtain an IP address for the interface (this enables DHCP on a Layer 3 SVI)
helper-address <IP>	Forwards DHCP and BOOTP packets • <IP> - Defines the IP to which DHCP and BOOTP packets are forwarded **NOTE:** IP helper addresses can only be applied on SVI but not on the physical interfaces.
nat [inside|outside]	Sets *Network Address Translation* (NAT) parameters • inside – Inside interface • outside – Outside interface
arp [rate-limit <1-1000000>| trust]	Sets arp for the packets • rate-limit <1-1000000> – Displays the allowed rate in packets per second • trust – Displays trust state for arp responses coming in this interface
dhcp trust	Sets dhcp trust state for dhcp responses coming in this interface

Usage Guidelines

IPv4 commands are not allowed on a L2 interface. Use the `ip access-group` command to attach an access list to an interface. Use the `no ip access-group` command to remove the access list from the interface

Use `mac access-group` to attach a MAC access list to an interface

Use the `{no} ip [options]` command to undo IP based interface configurations

Example

```
RFController(config-if)#ip access-group 110 in
RFController(config-if)#

RFController(config-if)#ip address 192.168.234.1/24
RFController(config-if)#
```

Creating helper address using DHCP server

Follow the steps below to create a helper address on VLAN 2000 for using a DHCP server on VLAN 1000:

```
RFController(config)#interface vlan 1000
RFController(config-if)#ip address 172.168.100.1/24

RFController(config-if)#interface vlan 2000
RFController(config-if)#ip address 172.168.200.1/24
RFController(config-if)#ip helper-address 172.168.100.10
RFController(config-if)#
```

Configuring a static NAT source translation

The example below displays static NAT source translation:

```
RFController(config)#interface vlan 1000
RFController(config-if)#ip nat inside

RFController(config-if)#interface vlan 2000
RFController(config-if)#ip nat outside

RFController(config)#ip nat inside source static 172.168.200.10 157.235.205.57
RFController(config)#
```

mac

Interface config commands

Applies a MAC access list (ACL) to Gigabit Ethernet interface

NOTE
The access list cannot be applied on a management interface (me1).

Supported in the following platforms:

- Mobility RFS4000 Controller
- Mobility RFS6000 Controller
- Mobility RFS7000 Controller

Syntax

```
mac access-group <acl-name> in
```

Parameters

access-group <acl-name>	Sets the MAC access groups ACL • <acl-name> – Sets ACL name • in – Applies the ACL to ingress packets

Example

```
RFController(config-if)#mac access-group Ark200 in
RFController(config-if)#
```

management

Interface config commands

Sets the selected interface as management interface. It can only be used on a VLANx interface. The TFTP/FTP server providing the controller its config file at startup must be accessible via this interface.

VLAN 1 is the default management interface for the controller.

Supported in the following platforms:

- Mobility RFS4000 Controller
- Mobility RFS6000 Controller
- Mobility RFS7000 Controller

Syntax

```
management
```

Parameters

None

Usage Guidelines

The management privilege can be set only on a L3 interface. Use this command along with the `(config) management secure` in the config mode. This ensure management access is restricted to the management VLAN only

Refer to *management on page 268* for `management` configuration.

Example

```
RFController(config)#interface vlan 1000
RFController(config-if)#management
RFController(config-if)#
```

no

Interface config commands

Negates a command or sets its defaults

Supported in the following platforms:

- Mobility RFS4000 Controller
- Mobility RFS6000 Controller
- Mobility RFS7000 Controller

NOTE
The following commands display only for the Mobility RFS6000 Controller and the Mobility RFS4000 Controller:
- power
The following commands display only for the Mobility RFS7000 Controller and the Mobility RFS4000 Controller:
- port-channel
- static-channel-group

Syntax

```
no [crypto|description|duplex|ip|mac|port-channel|
shutdown|spanning-tree|speed|static-channel-group|
storm-control|controllerport]
```

Parameters

The `no` command negates any command associated with it. Wherever required, use the same parameters associated with the command getting negated.

Example

```
RFController(config-if)#no duplex
RFController(config-if)#
```

port-channel

Interface config commands

Selects the load-balance criteria of an aggregated port

Supported in the following platforms:

- Mobility RFS7000 Controller
- Mobility RFS4000 Controller

NOTE
This command is not supported on the Mobility RFS6000 Controller.

Syntax

```
port-channel load-balance [src-dst-ip|src-dst-mac]
```

Parameters

load-balance [src-dst-ip|src-dst-mac]	Sets load-balancing for port channel • src-dst-ip – Defines the Source and Destination IP address based on the current load balancing • src-dst-mac – Sets the Source and Destination MAC address based on the load balancing

Usage Guidelines

Use this command to configure and set load balance on the aggregated port using `(config-if) static-channel-group`.

Example

The following example creates a channel group 1, with interface ge1 and ge 2:

```
RFController(config)#interface ge1
RFController(config-if)#static-channel-group 1

RFController(config)#interface ge2
RFController(config-if)#static-channel-group 1
```

The following example defines the load balance based on the IP or MAC address:

```
RFController(config)#interface sa1
RFController(config-if)#port-channel load-balance src--dst-ip
RFController(config-if)#
```

Configuring a port aggregation

Use `static-channel-group` and `port-channel` for configuring port aggregation. Follow the steps below to configure port aggregation:

1. Create a static channel group for port aggregation and associate an interface with it.

```
RFController(config)#interface ge 1
RFController(config-if)#static-channel-group 1
```

2. Execute `show static-channel-group` and ensure the virtual static aggregation sa 1 has been created and associated with `ge 1`.

3. Select the other interface required for port aggregation and associate the static channel group to it.

```
RFController(config)#interface ge 2
RFController(config-if)#static-channel-group 1
```

4. Execute `show static-channel-group` and ensure the virtual static aggregation sa 1 has been created and associated with `ge 2`.
   Both ge 1 and ge 2 are now aggregated and ready for use.

5. Use the `port-channel` command to select the criteria used to determine which link is selected for a given packet. The port-channel selection is based on either source-destination IP or source destination MAC

```
RFController(config-if)#port-channel load-balance src-dst-ip
RFController(config-if)#
```

The default port-channel criteria is based on source-destination IP. The port channel (when configured with `src-dst-ip)` does not show up in the running-config. Hence, this mode is preferred over `src-dst-mac`.

NOTE
When a port (GE) is aggregated into a *Static Aggregation* (SA), it temporarily takes on the port configuration of the SA.
For example, If GE 1 (previously configured as trunk vlan 1-10) and GE 2 (previously configured as trunk vlan 11-20) are now aggregated as SA 1 and SA 1 is configured as trunk vlan 100-200, then SA 1's configuration applies to both GE 1 and GE 2. This new configuration like VLAN, speed, duplex, MST is now applicable on the ports as long as they are part of the SA. The ports revert back to the original configuration once they are removed from the SA.

How src-dst-mac mode works

When the controller sends a packet out of a SA, it selects the egress port as a function of the packet's source MAC, destination MAC, and the set of ports in the SA which are running. It XORs the bottom bits of the two MACs and indexes it into a table of the running ports.

How src-dst-ip mode works

When the controller sends an IP packet, the egress port is chosen as a function of the packet's source IP, destination IP and the set of running ports. It XORs the bottom byte of the two IP addresses and indexes then into the same table of running ports that `src-dst-mac` mode uses.

If the packet is NOT an IP packet, it uses the same calculation as src-dst-mac mode.

Why is src-dst-ip mode preferred

src-dst-ip mode distributes packets better when most packets, going through the gateway, are IP packets. In the presence of an IP gateway, the IP packets forwarded from one Client to hosts that is beyond the gateway all have the same MAC pair <Client MAC, Gateway MAC> no matter what host the Client is accessing.

But in src-dst-mac balancing, the same link is selected always.

power

Interface config commands

Invokes PoE commands to configure PoE power limit and priority for a port. By default the value for a GE port is set to low. Power is applied in order of priority, power overlaods are removed in reverse order of priority.

Supported in the following platforms:

- Mobility RFS4000 Controller
- Mobility RFS6000 Controller

Syntax

```
power [limit <0-30>|priority {critical|high|low}]
```

Parameters

limit <0-30>	Sets the power limit on the given port to the stated power in Watts. Select the power limit value between 0-30 (Watts). It actually limits to 29.7W
priority [critical|high|low]	Sets PoE priority for port • critical – Sets the PoE priority as critical priority • high – Sets the PoE priority as high priority • low – Sets the PoE priority as low priority

Usage Guidelines

Use `[no] power` to rollback the PoE configurations and set back the default configuration

Example

```
RFController(config)#interface ge1
RFController(config-if)#no power
RFController(config-if)#exit
RFController(config)#interface ge2
RFController(config-if)#power limit 14
RFController(config-if)#exit
RFController(config)#interface ge3
RFController(config-if)#power priority critical
RFController(config-if)#exit
RFController(config)#show power configuration
Power usage trap at 80% of max power (148 of 185 Watts)
 port  Priority    Power limit  Enabled
  ge1  high        29.7W         no
  ge2  high        14.0W        yes
  ge3  crit        29.7W        yes
  ge4  high        29.7W        yes
  ge5  high        29.7W        yes
  ge6  high        29.7W        yes
  ge7  high        29.7W        yes
  ge8  high        29.7W        yes
 POE firmware version 01f6 build 4
RFController(config)#
```

service

Interface config commands

Invokes service commands to troubleshoot or debug the `(config-if)` instance configuration.

Supported in the following platforms:

- Mobility RFS4000 Controller
- Mobility RFS6000 Controller
- Mobility RFS7000 Controller

Syntax

```
service show cli
```

Parameters

cli	Displays the CLI tree of the current mode

Example

```
RFController(config-if)#service show cli
Interface Config mode:
+-clrscr [clrscr]
+-crypto
  +-map
    +-WORD [crypto map WORD]
+-description
  +-LINE [description LINE]
+-do
  +-LINE [do LINE]
+-duplex
  +-auto [duplex (half|full|auto)]
  +-full [duplex (half|full|auto)]
  +-half [duplex (half|full|auto)]
+-end [end]
+-exit [exit]
+-help [help]
+-ip
  +-access-group
    +-<1-99>
      +-in [ip access-group (<1-99>|<100-199>|<1300-1999>|<2000-2699>|WORD)
(in)]
    +-<100-199>
RFController(config-if)#
```

show

Interface config commands

Displays current system information running on the controller

Supported in the following platforms:

- Mobility RFS4000 Controller
- Mobility RFS6000 Controller
- Mobility RFS7000 Controller

NOTE
The following commands display only for the Mobility RFS6000 Controller and the Mobility RFS4000 Controller:
- power
The following commands display only for the Mobility RFS7000 Controller and the Mobility RFS4000 Controller:
- port-channel
- static-channel-group

Syntax

```
show <parameter>
```

Parameters

?	Displays the parameters for which information can be viewed using the show command

Example

```
RFController(config-if)#show ?
  aap-wlan-acl          wlan based acl
  aap-wlan-acl-stats    IP filtering wlan based statistics
  access-list           Internet Protocol (IP)
  aclstats              Show ACL Statistics information
  alarm-log             Display all alarms currently in the system
  autoinstall           autoinstall configuration
  banner                Display Message of the Day Login banner
  boot                  Display boot configuration.
  clock                 Display system clock
  commands              Show command lists
  crypto                encryption module
  debugging             Debugging information outputs
  dhcp                  DHCP Server Configuration
  environment           show environmental information
  file                  Display filesystem information
  firewall              Wireless firewall
  ftp                   Display FTP Server configuration
  history               Display the session command history
  interfaces            Interface status
  ip                    Internet Protocol (IP)
  ldap                  LDAP server
  licenses              Show any installed licenses
  logging               Show logging configuration and buffer
  mac                   Internet Protocol (IP)
  mac-address-table     Display MAC address table
```

```
  mac-name              Displays the configured MAC names
  management            Display L3 Managment Interface name
  mobility              Display Mobility parameters
  ntp                   Network time protocol
  password-encryption   password encryption
  port-channel          Portchannel commands
  privilege             Show current privilege level
  protocol-list         List of protocols
  radius                RADIUS configuration commands
  redundancy            Display redundancy group parameters
  role                  Configure role parameters
  rtls                  Real Time Locating System commands
  running-config        Current Operating configuration
  securitymgr           Securitymgr parameters
  service-list          List of services
  sessions              Display current active open connections
  snmp                  Display SNMP engine parameters
  snmp-server           Display SNMP engine parameters
  smtp-notification     Display SNMP engine parameters
  spanning-tree         Display spanning tree information
  startup-config        Contents of startup configuration
  static-channel-group  static channel group membership
  terminal              Display terminal configuration parameters
  timezone              Display timezone
  traffic-shape         Display traffic shaping
  upgrade-status        Display last image upgrade status
  users                 Display information about currently logged
                        in users
  version               Display software & hardware version
  wireless              Wireless configuration commands
  wlan-acl              wlan based acl
  wwan                  Wireless wan interface

RFController(config-if)#show
```

shutdown

Interface config commands

Disables the selected interface, the interface is administratively enabled unless explicitly disabled using this command

Displays current system information running on the controller

Supported in the following platforms:

- Mobility RFS4000 Controller
- Mobility RFS6000 Controller
- Mobility RFS7000 Controller

Syntax

```
shutdown
```

Parameters

None

Example

```
RFController(config-if)#shutdown
RFController(config-if)#
```

spanning-tree

Interface config commands

Configures spanning tree parameters

Displays current system information running on the controller.

Supported in the following platforms:

- Mobility RFS4000 Controller
- Mobility RFS6000 Controller
- Mobility RFS7000 Controller

Syntax

```
spanning-tree [bpdufilter|bpduguard|edgeport|force-version|
guard|link-type|mst|portfast]
spanning-tree bpdufilter [enable|disable]
spanning-tree bpduguard [enable|disable]
spanning-tree [edgeport|portfast]
spanning-tree force-version <1-3>
spanning-tree guard root
spanning-tree link-type [point-to-point|shared]
spanning-tree mst [<1-15|port-cisco]
spanning-tree mst 1 [cost <>|port-priority <>]
spanning-tree mst port-cisco [enable|disable]
```

Parameters

bpdufilter [disable|enable]	Use this command to set a portfast BPDU filter for the port. Use the no parameter with this command to revert the port BPDU filter to default. The spanning tree protocol sends BPDUs from all ports. Enabling the BPDU filter ensures PortFastenabled ports do not transmit or receive BPDUs.
bpduguard [disable|enable]	Use this command to enable or disable the BPDU guard feature on a port. Use the no parameter with this command to set the BPDU guard feature to default values. When the BPDU guard is set for a bridge, all portfast-enabled ports that have the BPDU-guard set to default shut down the port upon receiving a BPDU. If this occurs, the BPDU is not processed. The port can be brought back either manually (using the no shutdown command), or by configuring the errdisable-timeout to enable the port after the specified interval.
edgeport	Enables an interface as an edgeport
force-version <0-3>	Specifies the spanning-tree force version. A version identifier of less than 2 enforces the spanning tree protocol. Select from the following versions: • 0 – STP • 1 – Not supported • 2 – RSTP • 3 – MSTP The default value for forcing the version is MSTP
guard root	Enables the Root Guard feature for the port. The root guard disables the reception of superior BPDUs. The Root Guard ensures the enabled port is a designated port. If the Root Guard enabled port receives a superior BPDU, it moves to a discarding state. Use the no parameter with this command to disable the root guard feature.
link-type [point-to-point|shared]	Enables or disables point-to-point or shared link types • point-to-point – Enables rapid transition • shared – Disables rapid transition

mst [<0-15> [cost <1-200000000>| port-priority <0-240>]| port-cisco-interoperability [disable|enable]]	Configures MST values on a spanning tree
	• <0-15> [cost <1-200000000>|port-priority <0-240>] – Defines the Instance ID
	  • cost <1-200000000> – Defines the path cost for a port
	  • port-priority <0-240> – Defines the port priority for a bridge
	• port-cisco-interoperability [disable|enable] – Enables or disables interoperability with Cisco's version of MSTP (which is incompatible with standard MSTP).
	  • enable – Enables CISCO Interoperability
	  • disable – Disables CISCO Interoperability - The default value is disabled

portfast	Enables rapid transitions

Example

```
RFController(config-if)#spanning-tree edgeport
RFController(config-if)#
```

```
RFController(config-if)#spanning-tree guard root
RFController(config-if)#

RFController(config-if)#spanning-tree link-type point-to-point
RFController(config-if)#
```

speed

Interface config commands

Specifies the speed of a fast-ethernet (10/100) or a gigabit-ethernet port (10/100/1000)

Displays current system information running on the controller.

Supported in the following platforms:

- Mobility RFS4000 Controller
- Mobility RFS6000 Controller
- Mobility RFS7000 Controller

Syntax

```
speed [10|100|1000|auto]
```

Parameters]

10	Forces 10 Mbps operation
100	Forces 100 Mbps operation
1000	Forces 1000 Mbps operation
auto	Port automatically detects the speed it should run based on the port at the other end of the link.Autonegotiation is a requirement for using 1000BASE-T[3] according to the standard.

Usage Guidelines

Set the interface speed to auto to detect and use the fastest speed available. Speed detection is based on connected network hardware.

Example

```
RFController(config-if)#speed auto
RFController(config-if)#
```

static-channel-group

Interface config commands

Adds an interface to a static channel group

Displays current system information running on the controller.

Supported in the following platforms:

- Mobility RFS7000 Controller
- Mobility RFS4000 Controller

NOTE
The Mobility RFS6000 Controller does not support this command.

Syntax

```
static-channel-group <1-4>
```

Parameters

<1-4>	Sets a static channel group to associate the link with

Usage Guidelines

This command aggregates individual giga ports into a single aggregate link to provide greater bandwidth. The static channel group is used to provide additional bandwidth in multiples of 1Gbps on the controller. All MAC layer and higher protocols see only the static channel group (aggregate link) rather than the individual ports that comprise it.

Example

```
RFController(config-if)#static-channel-group 2
RFController(config-if)#
```

controllerport

Interface config commands

Sets controller mode characteristics for the selected interface.

Supported in the following platforms:

- Mobility RFS4000 Controller
- Mobility RFS6000 Controller
- Mobility RFS7000 Controller

Syntax

```
controllerport [access|mode|trunk]
controllerport access vlan <1-4094>
controllerport mode [access|trunk]
controllerport trunk [allowed|native]
controllerport trunk allowed vlan [add|none|remove] <vlan-id>
controllerport trunk native [tagged|vlan<1-4094>]
```

Parameters

access vlan <1-4094>	Configures the access vlan of an access-mode port • vlan <1-4094> – Sets the vlan when interface is in access mode
mode [access|trunk]	Sets the mode of the interface to access or trunk mode (can only be used on physical (layer2) interfaces) • access – If `access` mode is selected, the access vlan is automatically set to vlan1. In this mode, only untagged packets in the access vlan (vlan1) are accepted on this port. All tagged packets are discarded. • trunk – If `trunk` mode is selected, tagged vlan packets VLANs are accepted. The native vlan is automatically set to VLAN1. Untagged packets are placed in the native vlan by the controller. Outgoing packets in the native vlan are sent untagged.`trunk` is the default mode for both ports

trunk [allowed |native]	Sets the trunking mode characteristics
	• allowed vlan – Configures trunk characteristics when the port is in trunk-mode
	  • vlan [add|none|remove] – Sets allowed vlans
	  • none – Allows no vlans to Xmit/Rx through the Layer2 interface
	  • add – Adds vlans to the current list
	  • remove – Removes vlans from the current list
	  • <vlan-id> – vlan-ids added or removed. Can be either a range of vlans (55-60) or a list of comma separated vlan-ids (35, 41 etc.)
	• native [tagged|vlan <1-4094>] – Configures the native VLAN ID of the trunk-mode port
	  • tagged – Tags the native vlan
	  • vlan <1-4094> – Sets the native VLAN for classifying untagged traffic when the interface is in trunking mode

Usage Guidelines

Interfaces ge1-ge4 can be configured as trunk or in access mode. An interface (when configured as trunk) allows packets (from the given list of vlans) to be added to the trunk. An interface configured as "*access*" allows packets only from native vlans

Use the `[no] controllerport (access|mode|trunk)` to undo controllerport configurations

Example

```
RFController(config-if)#controllerport mode access
RFController(config-if)#
```

storm-control

Interface config commands

Sets storm-control for broadcasting

Supported in the following platforms:

- Mobility RFS4000 Controller
- Mobility RFS6000 Controller
- Mobility RFS7000 Controller

Syntax

```
storm-control [bcast|mcast|ucast] rate-limit <1-1000000>
```

Parameters

bcast rate-limit <1-1000000>	Configures storm-control of broadcast packets. • rate-limit <1-1000000> – Performs packet rate limiting • <1-1000000> – Displays allowed rate in packets per second
mcast rate-limit <1-1000000>	Configures storm-control of multicast packets. • rate-limit <1-1000000> – Performs packet rate limiting • <1-1000000> – Displays allowed rate in packets per sec ond
ucast rate-limit <1-1000000>	Configures storm-control of unicast packets • rate-limit <1-1000000> – Performs packet rate limiting • <1-1000000> – Displays allowed rate in packets per sec ond

Example

```
RFController(config-if)#storm-control bcast ratelimit 88
RFController(config-if)#
RFController(config-if)#storm-control mcast ratelimit 88
RFController(config-if)#
RFController(config-if)#storm-control ucast ratelimit 88
RFController(config-if)#
```

tunneling

Interface config commands

Sets protocol-over protocol tunneling.

Supported in the following platforms:

- Mobility RFS4000 Controller
- Mobility RFS6000 Controller
- Mobility RFS7000 Controller

Syntax

```
tunnel [destination <A.B.C.D>|source <A.B.C.D>|ttls <1-255>]
```

Parameters

destination <A.B.C.D>	Destination of the tunnel packet. • <A.B.C.D> – Specifies the IP address of the destination.
source <A.B.C.D>	Source of tunnel packets. • <A.B.C.D> – Specifies the IP address of the source.
ttl<1-255>	Sets time to live.

Example

```
RFController(config-if)#tunnel destination 1.2.6.3
RFController(config-if)#
```

Chapter

13

Spanning tree-mst Instance

In this chapter

Use the `(config-mst)` instance to configure the controllers *Multi Spanning Tree Protocol* (MSTP) configuration. To switch to this instance, use the command:

```
RFController(config)#spanning-tree mst configuration
RFController(config-mst)#
```

mst config commands

Table summarizes the **`(config-mst)`** commands:

TABLE 13 MSTI Configuration Commands

Command	Description	Ref.
clrscr	Clears the display screen	*page 436*
end	Ends the current mode and moves to the EXEC mode	*page 437*
exit	Ends the current mode and moves to the previous mode	*page 438*
help	Displays the system's interactive help system	*page 439*
instance	Assigns a VLAN to the bridge instance	*page 440*
name	Sets a name for the MST region	*page 441*
no	Negates a command or sets defaults	*page 442*
revision	Configures the revision number of the MST bridge	*page 443*
service	Invokes service commands needed to troubleshoot or debug `(config-if)` instance configurations	*page 444*
show	Shows running system information	*page 446*

clrscr

mst config commands

Clears the display

Supported in the following platforms:

- Mobility RFS4000 Controller
- Mobility RFS6000 Controller
- Mobility RFS7000 Controller

Syntax

```
clrscr
```

Parameters

None

Example

```
RFController(config-mst)#clrscr
RFController(config-mst)#
```

end

mst config commands

Ends and exits the current mode and moves to the PRIV EXEC mode. The prompt changes to `RFController#`

Supported in the following platforms:

- Mobility RFS4000 Controller
- Mobility RFS6000 Controller
- Mobility RFS7000 Controller

Syntax

```
end
```

Parameters

None

Example

```
RFController(config-mst)#end
RFController#
```

exit

mst config commands

Ends the current mode and moves to the previous mode (GLOBAL-CONFIG). The prompt changes to `RFController(config)#`

Supported in the following platforms:

- Mobility RFS4000 Controller
- Mobility RFS6000 Controller
- Mobility RFS7000 Controller

Syntax

```
exit
```

Parameters

None

Example

```
RFController(config-mst)#exit
RFController(config)#
```

help

mst config commands

Displays the system's interactive help system

Supported in the following platforms:

- Mobility RFS4000 Controller
- Mobility RFS6000 Controller
- Mobility RFS7000 Controller

Syntax

```
help
```

Parameters

None

Example

```
RFController(config-mst)#help
CLI provides advanced help feature. When you need help,
anytime at the command line please press '?'.

If nothing matches, the help list will be empty and you must backup
until entering a '?' shows the available options.
Two styles of help are provided:
1. Full help is available when you are ready to enter a
   command argument (e.g. 'show ?') and describes each possible
   argument.
2. Partial help is provided when an abbreviated argument is entered
   and you want to know what arguments match the input
   (e.g. 'show ve?'.)

RFController(config-mst)#
```

instance

mst config commands

Associates VLAN(s) with an instance

Supported in the following platforms:

- Mobility RFS4000 Controller
- Mobility RFS6000 Controller
- Mobility RFS7000 Controller

Syntax

```
instance <1-15> vlan <vlan-id>
```

Parameters

<1-15>	Defines the instance ID to which the VLAN is associated
vlan <vlan-id>	Sets the VLAN ID for its association with an instance

Usage Guidelines

MSTP works based on instances. An instance is a group of VLANs with a common spanning tree. A single VLAN cannot be associated with multiple instances.

Controllers with the same instance, VLAN mapping, revision number and region names define a unique region. Controllers in the same region exchange *bridge protocol data units* (BPDUs) with instance record information within it.

Example

The following example sets an instance named 10 and maps VLAN 20 to it:

```
RFController(config-mst)#instance 10 vlan 20
RFController(config-mst)#
```

name

mst config commands

Sets the name for the MST region

Supported in the following platforms:

- Mobility RFS4000 Controller
- Mobility RFS6000 Controller
- Mobility RFS7000 Controller

Syntax

```
name <region-name>
```

Parameters

<region-name>	Sets MST region name

Example

```
RFController(config-mst)#name MyRegion
RFController(config-mst)#
```

no

mst config commands

Negates a command or sets its defaults

Supported in the following platforms:

- Mobility RFS4000 Controller
- Mobility RFS6000 Controller
- Mobility RFS7000 Controller

Syntax

```
no [instance|name|revision]
```

Parameters

instance	Sets the MST Instance • vlan – Delete the association of vlan with this instance • <vlan-id> – List of vlan IDs
name	Assigns a name to the MST region
revision	Defines the revision number for configuration information

Usage Guidelines

The `no` command negates any command associated with it. Wherever required, use the same parameters associated with the command getting negated.

Example

```
RFController(config-mst)#no instance 10 vlan 20
RFController(config-mst)#

RFController(config-mst)#no name MyRegion
RFController(config-mst)#

RFController(config-mst)#no revision
RFController(config-mst)#
```

revision

mst config commands

Sets the revision number of the MST bridge

Supported in the following platforms:

- Mobility RFS4000 Controller
- Mobility RFS6000 Controller
- Mobility RFS7000 Controller

Syntax

```
revision <0-255>
```

Parameters

revision <0-255>	Defines the revision number for configuration information

Example

```
RFController(config-mst)#revision 20
RFController(config-mst)#
```

service

mst config commands

Invokes service commands needed to troubleshoot or debug `(config-if)` instance configurations

Supported in the following platforms:

- Mobility RFS4000 Controller
- Mobility RFS6000 Controller
- Mobility RFS7000 Controller

Syntax

```
service show cli
```

Parameters

None

Example

```
RFController(config-mst)#service show cli
MSTI configuration mode:
+-clrscr [clrscr]
+-end [end]
+-exit [exit]
+-help [help]
+-instance
  +-<1-15> [instance <1-15>]
    +-vlan
      +-VLAN_ID [instance <1-15> vlan VLAN_ID]
+-name
  +-LINE [name LINE]
+-no
  +-instance
    +-<1-15> [no instance <1-15>]
      +-vlan
        +-VLAN_ID [no instance <1-15> vlan VLAN_ID]
  +-name [no name]
  +-revision [no revision]
+-quit [quit]
+-revision
  +-REVISION_NUM [revision REVISION_NUM]
+-s
  +-commands [show commands]
    +-WORD [show commands WORD]
  +-running-config [show running-config]
    +-full [show running-config full]
    +-include-factory [show running-config include-factory]
+-service
  +-show
    +-cli [service show cli]
+-show
  +-access-list [show access-list]
    +-<1-99> [show access-list
(<1-99>|<100-199>|<1300-1999>|<2000-2699>|WORD)]
    +-<100-199> [show access-list
(<1-99>|<100-199>|<1300-1999>|<2000-2699>|WORD)]
```

```
    +-<1300-1999> [show access-list
(<1-99>|<100-199>|<1300-1999>|<2000-2699>|WORD)]
    +-<2000-2699> [show access-list
(<1-99>|<100-199>|<1300-1999>|<2000-2699>|WORD)]
    +-WORD [show access-list (<1-99>|<100-199>|<1300-1999>|<2000-2699>|WORD)]
  +-aclstats
    +-vlan
      +-<1-4094> [show aclstats ( vlan <1-4094> )].................
.................................................................
.................................................................

RFController(config-mst)#
```

show

mst config commands

Displays current system information

Supported in the following platforms:

- Mobility RFS4000 Controller
- Mobility RFS6000 Controller
- Mobility RFS7000 Controller

NOTE
The following commands display only for the Mobility RFS6000 Controller and the Mobility RFS4000 Controller:
- power
The following commands display only for the Mobility RFS7000 Controller and the Mobility RFS4000 Controller:
- port-channel
- static-channel-group

Syntax

```
show <parameter>
```

Parameters

parameter	Displays the parameters for which information can be viewed using the show command

Example

```
RFController(config-mst)#show ?
  access-list           Internet Protocol (IP)
  aclstats              Show ACL Statistics information
  alarm-log             Display all alarms currently in the system
  autoinstall           autoinstall configuration
  banner                Display Message of the Day Login banner
  boot                  Display boot configuration.
  clock                 Display system clock
  commands              Show command lists
  crypto                encryption module
  debugging             Debugging information outputs
  dhcp                  DHCP Server Configuration
  environment           show environmental information
  file                  Display filesystem information
  firewall              Wireless firewall
  ftp                   Display FTP Server configuration
  history               Display the session command history
  interfaces            Interface status
  ip                    Internet Protocol (IP)
  ldap                  LDAP server
  licenses              Show any installed licenses
  logging               Show logging configuration and buffer
  mac                   Internet Protocol (IP)
  mac-address-table     Display MAC address table
  mac-name              Displays the configured MAC names
  management            Display L3 Managment Interface name
```

```
  mobility              Display Mobility parameters
  ntp                   Network time protocol
  password-encryption   password encryption
  port                  Physical/Aggregate port interface
  port-channel          Portchannel commands
  privilege             Show current privilege level
  radius                RADIUS configuration commands
  redundancy            Display redundancy group parameters
  role                  Configure role parameters
  rtls                  Real Time Locating System commands
  running-config        Current Operating configuration
  securitymgr           Securitymgr parameters
  sessions              Display current active open connections
  snmp                  Display SNMP engine parameters
  smtp-notification      Display SNMP engine parameters
  snmp-server           Display SNMP engine parameters
  spanning-tree         Display spanning tree information
  startup-config        Contents of startup configuration
  static-channel-group  static channel group membership
  terminal              Display terminal configuration parameters
  timezone              Display timezone
  traffic-shape         Display traffic shaping
  upgrade-status        Display last image upgrade status
  users                 Display information about currently logged
                        in users
  version               Display software & hardware version
  virtual-ip            IP redundancy feature
  wireless              Wireless configuration commands
  wlan-acl              wlan based acl
  wwan                  Wireless wan interface
RFController(config-mst)#show
```

Chapter

14 Extended ACL Instance

In this chapter

The Extended ACL instance `(config-ext-nacl)` is used to manage the extended Access Control List entries associated with the controller.

To navigate to this instance, use the command

```
RFController(config)#ip access-list extended [<ACL-name>|
       <100-199>|<2000-2699>]
RFController(config-ext-nacl)#
```

Extended ACL config commands

Table 14 summarizes **`config-ext-nacl`** commands:

TABLE 14 Extended ACL Config Command Summary

Command	Description	Ref.
clrscr	Clears the display screen	*page 450*
deny	Specifies packets to reject	*page 451*
exit	Ends the current mode and moves to the previous mode	*page 456*
help	Displays the interactive help system	*page 457*
mark	Specifies packets to mark	*page 458*
no	Negates a command or sets its defaults	*page 462*
permit	Specifies packets to forward	*page 463*
service	Invokes the service commands to troubleshoot or debug `(config-if)` instance configurations	*page 467*
show	Displays running system information	*page 468*

clrscr

Extended ACL config commands

Clears the display screen

Supported in the following platforms:

- Mobility RFS4000 Controller
- Mobility RFS6000 Controller
- Mobility RFS7000 Controller

Syntax

```
clrscr
```

Parameters

None

Example

```
RFController(config-ext-nacl)#clrscr
RFController(config-ext-nacl)#
```

deny

Extended ACL config commands

Specifies packets to reject

Supported in the following platforms:

- Mobility RFS4000 Controller
- Mobility RFS6000 Controller
- Mobility RFS7000 Controller

Syntax

```
deny [icmp|ip|tcp|upd|proto]

deny icmp [<source-IP/Mask>|any|host <IP>] [<dest-IP/Mask>|any|host <IP>]
{<ICMP-type> {<ICMP-code>}} {log} {rule-precedence <1-5000>}

deny ip [<source-IP/Mask>|any|host <IP>] [<dest-IP/Mask>|any|host <IP>] {log}
{rule-precedence <1-5000>}

deny [tcp|udp] [<source-IP/Mask>|any|host <IP>] {eq
<source-port>|range <starting-source-port>
<ending-source-port>} [<dest-IP/Mask|any|host <IP>]
{eq <source-port>} {range <starting-source-port>
<ending-source-port>} {log} {rule-precedence <1-5000>}

deny proto [<1-254>|WORD|eigrp|gre|igmp|igp|ospf|vrrp]
             [<source-IP/Mask>|any|host <IP>][<dest-IP/Mask>|any|host <IP>]
              {log} {rule-description<WORD>|rule-precedence<1-5000>}
```

Parameters

deny ip [<source-IP/Mask>|any|host <IP>][<dest-IP/Mask>|any|host <IP>] *{log} {rule-precedence <1-5000>}*	Use with a **deny** command to reject IP packets • deny – Sets the action type on an ACL • ip – Specifies an IP (to match to a protocol) • <source-ip/mask>|any|host <IP> – The keyword <source-IP> is the source IP address of the network or host in dotted decimal format. The <Mask> is the network mask. For example, 10.1.1.10/24 indicates the first 24 bits of the source IP is used for matching. • any – any is an abbreviation for a source IP of 0.0.0.0 and source-mask bits equal to 0 • host – host is an abbreviation for the exact source <ip> (A.B.C.D format) and source-mask bits equal to 32 • <dest-IP/Mask>|any|host <IP> – Defines the destination host IP address or destination network address. • log – Generates log messages when the packet coming from the interface matches an ACL entry. Log messages are generated only for router ACLs. • rule-precedence <1-5000> – Defines an integer value between 1-5000. This value sets the rule precedence in the ACL.
deny icmp [<source-IP/Mask>|any|host <IP>] [<dest-IP/Mask>|any|host <IP>] *{<ICMP-type> {<ICMP-code>}} {log} {rule-precedence <1-5000>}*	Use with the **deny** command to reject ICMP packets • deny – Rejects ICMP packets • icmp – Specifies ICMP as the protocol • [<source-ip/mask>|any|host <IP>] – The source <source-IP> is the source IP address of the network or host (in dotted decimal format). The <mask> is the network mask. For example, 10.1.1.10/24 indicates the first 24 bits of the source IP is used for matching. • any – any is an abbreviation for a source IP of 0.0.0.0 and source-mask bits equal to 0 • host – host is an abbreviation for exact source (A.B.C.D) and source-mask bits equal to 32 • [<dest-IP/Mask>|any|host <IP>] – Defines the destination host IP address or destination network address • <ICMP-type> {<ICMP-code>} – Sets the ICMP type value <ICMP-type> from 0 to 255, and is valid only for ICMP. The ICMP code value <ICMP-code> is from 0 to 255, and is valid only for protocol type icmp. • log – Generates log messages when the packet coming from the interface matches the ACL entry. Log messages are generated only for router ACLs. • rule-precedence <1-5000> – Optional. Defines an integer value between 1-5000. This value sets the rule precedence in the ACL.

deny [tcp|udp] [<source-IP/Mask>|any|host <IP>] *{eq <source-port>|range <starting-source-port> <ending-source-port>}* [<dest-IP/Mask|any|host <IP>]*{eq <source-port>} {range <starting-source-port> <ending-source-port>} {log} {rule-precedence <1-5000>}*	Use with the **deny** command to reject TCP or UDP packets • deny – Rejects TCP or UDP packets • tcp|udp – Specifies TCP or UDP as the protocol • <source-IP/Mask>|any|host <IP> – The source is the source IP address of the network or host (in dotted decimal format). The source-mask is the network mask. For example, 10.1.1.10/24 indicates the first 24 bits of the source IP are used for matching. • any – any is an abbreviation for a source IP of 0.0.0.0, and the source-mask bits are equal to 0 • host – host is an abbreviation for exact source (A.B.C.D) and the source-mask bits equal to 32 • eq <source-port> – The source port <source-port> to match. Values in the range 1 to 65535. • range <starting-source-port> <ending-source-port> – Specifies the protocol range (starting and ending protocol numbers) • <dest-IP/Mask|any|host <IP> – Defines the destination host IP address or destination network address • eq <source-port>} {range <starting-source-port> <ending-source-port> – Specifies the destination port or range of ports. Port values are in the range of 1 to 65535. • log – Generates log messages when the packet coming from the interface matches the ACL entry. Log messages are generated only for router ACLs. • rule-precedence <1-5000> – Defines an integer value between 1-5000. This value sets the rule precedence in the ACL.

Usage Guidelines

Use this command to deny traffic between networks/hosts based on the protocol type selected in the access list configuration. The following protocol types are supported:

- ip
- icmp
- tcp
- udp

The last ACE in the access list is an implicit deny statement.

Whenever the interface receives the packet, its content is checked against the ACEs in the ACL. It is allowed/denied based on the ACL configuration.

- Filtering TCP/UDP allows the user to specify port numbers as filtering criteria
- Select the ICMP as the protocol to allow/deny ICMP packets. Selecting icmp provides the option of filtering icmp packets based on icmp type and code

NOTE
The log option is functional only for router ACL's. The log option displays an informational logging message about the packet that matches the entry sent to the console.

Example - denying traffic between two subnets

The following example denies traffic between two subnets:

```
RFController(config-ext-nacl)#deny ip 192.168.2.0/24 192.168.1.0/24
RFController(config-ext-nacl)#permit ip any any
RFController(config-ext-nacl)#
```

Example - denying TCP based traffic

The following example denies TCP traffic with a source port range between 20 - 23 (from the source subnet to destination subnet):

```
RFController(config-ext-nacl)#deny tcp range 20 23 192.168.1.0/24
192.168.2.0/24

RFController(config-ext-nacl)#permit ip any any
RFController(config-ext-nacl)#
```

Example - denying UDP based traffic

The following example denies UDP traffic with a source port range between 20 - 23 (from the source subnet to destination subnet):

```
RFController(config-ext-nacl)#deny udp range 20 23 192.168.1.0/24
192.168.2.0/24

RFController(config-ext-nacl)#permit ip any any
RFController(config-ext-nacl)#
```

Example - denying ICMP based traffic

The following example denies ICMP traffic from any source to any destination. The keyword *any* is used to match:

```
any source or destination IP address.
RFController(config-ext-nacl)#deny icmp any any
RFController(config-ext-nacl)#permit ip any any
RFController(config-ext-naclend
```

Example - denying protocol based ACL

With the inclusion of protocol based acls, it is possible to permit or deny all the protocols that exist.

```
RFController(config-ext-nacl)#deny proto ospf any any rule-precedence 10
RFController(config-ext-nacl)#deny proto eigrp any any rule-precedence 20
RFController(config-ext-nacl)#permit ip any any rule-precedence 30
```

end

Extended ACL config commands

Ends and exits the current mode and moves to the PRIV EXEC mode

The prompt changes to `RFController#`

Supported in the following platforms:

- Mobility RFS4000 Controller
- Mobility RFS6000 Controller
- Mobility RFS7000 Controller

Syntax

```
end
```

Parameters

None

Example

```
RFController(config-ext-nacl)#end
RFController#
```

exit

Extended ACL config commands

Ends the current mode and moves to the previous mode (GLOBAL-CONFIG). The prompt changes to `RFController(config)#`

Supported in the following platforms:

- Mobility RFS4000 Controller
- Mobility RFS6000 Controller
- Mobility RFS7000 Controller

Syntax

```
exit
```

Parameters

None

Example

```
RFController(config-ext-nacl)#exit
RFController(config)#
```

help

Extended ACL config commands

Displays the system's interactive help system

Supported in the following platforms:

- Mobility RFS4000 Controller
- Mobility RFS6000 Controller
- Mobility RFS7000 Controller

Syntax

```
help
```

Parameters

None

Example

```
RFController(config-ext-nacl)#help
CLI provides advanced help feature.  When you need help,
anytime at the command line please press '?'.

If nothing matches, the help list will be empty and you must backup
until entering a '?' shows the available options.
Two styles of help are provided:
1. Full help is available when you are ready to enter a
   command argument (e.g. 'show ?') and describes each possible
   argument.
2. Partial help is provided when an abbreviated argument is entered
   and you want to know what arguments match the input
   (e.g. 'show ve?'.)

RFController(config-ext-nacl)#
```

mark

Extended ACL config commands

Specifies packets to mark

Supported in the following platforms:

- Mobility RFS4000 Controller
- Mobility RFS6000 Controller
- Mobility RFS7000 Controller

Syntax

mark [8021p|dscp|tos]

mark [8021p <vlan-priority-value>|dscp
<dscp-codepoint-value>|tos <tos-value>] [icmp|ip|tcp|udp]

mark [8021p <vlan-priority-value>|dscp <dscp-codepoint-value>|tos <tos-value>]
icmp [<source-ip/mask>|any|host <ip>] [<dest-ip/mask>|any|host <ip>]
{<ICMP-type> {<ICMP-code>}} {log} {rule-precedence <1-5000>]}

mark [8021p <vlan-priority-value>|dscp <dscp-codepoint-value>|tos <tos-value>]
ip [<source-ip/mask>|any|host <ip>] [<dest-ip/mask>|any|host <ip>] *{log}*
{rule-precedence <1-5000>}

mark [8021p <vlan-priority-value>|dscp <dscp-codepoint-value>|tos <tos-value>]
[tcp|udp] [<source-ip/mask>|any|host <ip>] *{eq <source-port>|range*
<starting-source-port> <ending-source-port>} [<dest-ip/mask|any|host <ip>] *{eq*
<source-port>} {range <starting-source-port> <ending-source-port>} {log}
{rule-precedence <1-5000>}

Parameters

8021p <vlan-priority-value>	Sets the 802.1p VLAN user priority value to <vlan-priority-value> (0-7).
dscp <dscp-codepoint-value>	Sets the Differentiated Services Code Point code-point value to <dscp-codepoint-value> (0-63)
tos <tos-value>	Sets the TOS value to <tos-value>. The least significant two bits of the <tos-value> must be 0.

ip [<source-IP/Mask>|any|host <IP>] [<dest-IP/Mask>|any|host <IP>] *{log} {rule-precedence <1-5000>}*	Use with **mark** command to mark a packet. • ip – Specifies an IP (to match to a protocol) • <source-IP/Mask>|any|host <IP> – The keyword <source-IP> is the source IP address of the network or host in dotted decimal format. The <mask> is the network mask. For example, 10.1.1.10/24 indicates the first 24 bits of the source IP is used for matching. • any – any is an abbreviation for a source IP of 0.0.0.0 and source-mask bits equal to 0 • host – host is an abbreviation for the exact source <IP> (A.B.C.D format) and source-mask bits equal to 32 • <dest-IP/Mask>|any|host <IP> – Defines the destination host IP address or destination network address. • log – Generates log messages when the packet coming from the interface matches an ACL entry. Log messages are generated only for router ACLs. • rule-precedence <1-5000> – Defines an integer value between 1-5000. This value sets the rule precedence in the ACL.

icmp [<source-IP/mask>|any|host <IP>] [<dest-IP/Mask>|any|host <IP>] *{<ICMP-type> {<ICMP-code>}} {log} {rule-precedence <1-5000>]}*	Use with the **mark** command to mark ICMP packets • deny – Rejects ICMP packets • icmp – Specifies ICMP as the protocol • [<source-IP/mask>|any|host <IP>] – The source <source-IP> is the source IP address of the network or host (in dotted decimal format). The <Mask> is the network mask. For example, 10.1.1.10/24 indicates the first 24 bits of the source IP is used for matching. • any – any is an abbreviation for a source IP of 0.0.0.0 and source-mask bits equal to 0 • host – host is an abbreviation for exact source (A.B.C.D) and source-mask bits equal to 32 • [<dest-IP/Mask>|any|host <IP>] – Defines the destination host IP address or destination network address • <ICMP-type> {<ICMP-code>} – Sets the ICMP type value <ICMP-type> from 0 to 255, and is valid only for ICMP. The ICMP code value <ICMP-code> is from 0 to 255, and is valid only for protocol type icmp. • log – Generates log messages when the packet coming from the interface matches the ACL entry. Log messages are generated only for router ACLs. • rule-precedence <1-5000> – Defines an integer value between 1-5000. This value sets the rule precedence in the ACL.

[tcp|udp] [<source-IP/Mask>|any|host <IP>] {eq <source-port>|range <starting-source-port> <ending-source-port>} [<dest-IP/Mask|any|host <IP>] {eq <source-port>} {range <starting-source-port> <ending-source-port>} {log} {rule-precedence <1-5000>}	Use with the **mark** command to mark TCP or UDP packets • deny – Rejects TCP or UDP packets • tcp|udp – Specifies TCP or UDP as the protocol • <source-IP/Mask>|any|host <IP> – The source is the source IP address of the network or host (in dotted decimal format). The source-mask is the network mask. For example, 10.1.1.10/24 indicates the first 24 bits of the source IP are used for matching. • any – any is an abbreviation for a source IP of 0.0.0.0, and the source-mask bits are equal to 0 • host – host is an abbreviation for exact source (A.B.C.D) and the source-mask bits equal to 32 • eq <source-port> – The source port <source-port> to match. Values in the range 1 to 65535. • range <starting-source-port> <ending-source-port> – Specifies the protocol range (starting and ending protocol numbers) • <dest-IP/Mask|any|host <IP> – Defines the destination host IP address or destination network address • eq <source-port>} {range <starting-source-port> <ending-source-port> – Specifies the destination port or range of ports. Port values are in the range of 1 to 65535. • log – Generates log messages when the packet coming from the interface matches the ACL entry. Log messages are generated only for router ACLs. • rule-precedence <1-5000> – Defines an integer value between 1-5000. This value sets the rule precedence in the ACL.

Usage Guidelines

Marks traffic between networks/hosts based on the protocol type selected in the access list configuration

Use the mark option to specify the t*ype of service* (tos) and priority value. The tos value is marked in the IP header and the 802.1p priority value is marked in the dot1q frame.

The following types of protocols are supported:

- ip
- icmp
- tcp
- udp

Whenever the interface receives the packet, its content is checked against all ACEs in the ACL. It is marked based on the ACL configuration

- Filtering protocol types TCP/UDP allow the user to specify port numbers as filtering criteria
- Select ICMP to allow/deny ICMP packets (selecting ICMP allows you to filter packets based on the ICMP type and code)

NOTE
The log option is functional only for router ACL's. The log option provides an informational logging message about the packet matching the entry sent to the console.

Example - marking dot1p on TCP based traffic

The example below marks the dot1p priority value in the ethernet header to 5 on all TCP traffic coming from the source subnet:

```
RFController(config-ext-nacl)# mark 8021p 6 udp 192.168.2.0/24 range 5060 5061
RFController(config-ext-nacl)#
```

Example - marking tos on TCP based traffic

The example below marks the tos value in the IP header to 245 on all tcp traffic coming from the source subnet:

```
RFController(config-ext-nacl)# mark tos 160 udp 192.168.2.0/24 range 5060 5061
RFController(config-ext-nacl)#

RFController(config-ext-nacl)# mark dscp 40 udp 192.168.2.0/24 range 5060 5061
RFController(config-ext-nacl)#
```

no

Extended ACL config commands

Negates a command or sets its defaults

Supported in the following platforms:

- Mobility RFS4000 Controller
- Mobility RFS6000 Controller
- Mobility RFS7000 Controller

Syntax

```
no [deny|mark|permit]
```

Parameters

deny	Specifies packets to reject
mark	Specifies packets to mark
permit	Specifies packets to forward

Usage Guidelines

```
Removes an access list control entry. Provide the rule-precedence value when
using the no command.
```

Example

```
RFController(config-ext-nacl)#no mark 8021p 5 tcp 192.168.2.0/24 any
rule-precedence 10
RFController(config-ext-nacl)#

RFController(config-ext-nacl)#no permit ip any any rule-precedence 10
RFController(config-ext-nacl)#

RFController(config-ext-nacl)#no deny icmp any any rule-precedence 10
RFController(config-ext-nacl)#
```

permit

Extended ACL config commands

Permits specific packets.

NOTE
ACLs do not allow DHCP messages to flow by default. Configure an *Access Control Entry* (ACE) to allow DHCP messages to flow through.

```
RFController(config-ext-nacl)#permit ip xxx.xxx.xxx.xxx/x 192.168.2.0/24

RFController(config-ext-nacl)#permit ip any host xxx.xxx.xxx.xxx

RFController(config-ext-nacl)#
```

Supported in the following platforms:

- Mobility RFS4000 Controller
- Mobility RFS6000 Controller
- Mobility RFS7000 Controller

Syntax

permit[icmp|ip|tcp|upd|proto]

permit icmp [<source-IP/Mask>|any|host <ip>] [<dest-IP/Mask>|any|host <IP>] *{<ICMP-type> {<ICMP-code>}} {log} {rule-precedence <1-5000>]}*

permit ip [<source-IP/Mask>|any|host <IP>] [<dest-IP/mask>|any|host <IP>] *{log} {rule-precedence <1-5000>}*

permit [tcp|udp] [<source-ip/mask>|any|host <IP>] *{eq <source-port>|range <starting-source-port> <ending-source-port>}* [<dest-IP/Mask|any|host <IP>] *{eq <source-port>} {range <starting-source-port> <ending-source-port>} {log} {rule-precedence <1-5000>}*

permit proto [<1-254>|WORD|eigrp|gre|igmp|igp|ospf|vrrp]
[<source-IP/Mask>|any|host <IP>][<dest-IP/Mask>|any|host <IP>]
{log} {rule-description<WORD>|rule-precedence<1-5000>}

Parameters

permit ip [<source-IP/Mask>|any|host <IP>] [<dest-IP/mask>|any|host <IP>] *{log} {rule-precedence <1-5000>}*	Use with a **permit** command to allow IP packets • deny – Sets the action type on an ACL • IP – Specifies an IP (to match to a protocol) • <source-IP/Mask>|any|host <IP> – The keyword <source-IP> is the source IP address of the network or host in dotted decimal format. The <Mask> is the network mask. For example, 10.1.1.10/24 indicates the first 24 bits of the source IP is used for matching. • any – any is an abbreviation for a source IP of 0.0.0.0 and source-mask bits equal to 0 • host – host is an abbreviation for the exact source <IP> (A.B.C.D format) and source-mask bits equal to 32 • <dest-IP/Mask>|any|host <IP> – Defines the destination host IP address or destination network address. • log – Generates log messages when the packet coming from the interface matches an ACL entry. Log messages are generated only for router ACLs. • rule-precedence <1-5000> – Defines an integer value between 1-5000. This value sets the rule precedence in the ACL.
permit icmp [<source-IP/Mask>|any|host <ip>] [<dest-IP/Mask>|any|host <IP>] *{<ICMP-type> {<ICMP-code>}} {log} {rule-precedence <1-5000>]}*	Use with the **permit** command to allow ICMP packets • deny – Rejects ICMP packets • icmp – Specifies ICMP as the protocol • [<source-IP/Mask>|any|host <IP>] – The source <source-IP> is the source IP address of the network or host (in dotted decimal format). The <Mask> is the network mask. For example, 10.1.1.10/24 indicates the first 24 bits of the source IP is used for matching. • any – any is an abbreviation for a source IP of 0.0.0.0 and source-mask bits equal to 0 • host – host is an abbreviation for exact source (A.B.C.D) and source-mask bits equal to 32 • [<dest-IP/Mask>|any|host <IP>] – Defines the destination host IP address or destination network address • <ICMP-type> {<ICMP-code>} – Sets the ICMP type value <ICMP-type> from 0 to 255, and is valid only for ICMP. The ICMP code value <ICMP-code> is from 0 to 255, and is valid only for protocol type icmp. • log – Generates log messages when the packet coming from the interface matches the ACL entry. Log messages are generated only for router ACLs. • rule-precedence <1-5000> – Defines an integer value between 1-5000. This value sets the rule precedence in the ACL.

permit [tcp|udp] [<source-ip/mask>|any|host <IP>] *{eq <source-port>|range <starting-source-port> <ending-source-port>}* [<dest-IP/Mask|any|host <IP>] *{eq <source-port>} {range <starting-source-port> <ending-source-port>} {log} {rule-precedence <1-5000>}*	Use with the **permit** command to allow TCP or UDP packets • deny – Rejects TCP or UDP packets • tcp|udp – Specifies TCP or UDP as the protocol • <source-IP/Mask>|any|host <IP> – The source is the source IP address of the network or host (in dotted decimal format). The source-mask is the network mask. For example, 10.1.1.10/24 indicates the first 24 bits of the source IP are used for matching. • any – any is an abbreviation for a source IP of 0.0.0.0, and the source-mask bits are equal to 0 • host – host is an abbreviation for exact source (A.B.C.D) and the source-mask bits equal to 32 • eq <source-port> – The source port <source-port> to match. Values in the range 1 to 65535. • range <starting-source-port> <ending-source-port> – Specifies the protocol range (starting and ending protocol numbers) • <dest-IP/mask|any|host <IP> – Defines the destination host IP address or destination network address • eq <source-port>} {range <starting-source-port> <ending-source-port> – Specifies the destination port or range of ports. Port values are in the range of 1 to 65535. • log – Generates log messages when the packet coming from the interface matches the ACL entry. Log messages are generated only for router ACLs. • rule-precedence <1-5000> – Defines an integer value between 1-5000. This value sets the rule precedence in the ACL.

Use this command to permit traffic between networks/hosts based on the protocol type selected in the access list configuration. The following protocols are supported:

- ip
- icmp
- tcp
- udp

The last ACE in the access list is an implicit deny statement.

Whenever the interface receives the packet, its content is checked against all the ACEs in the ACL. It is allowed based on the ACL configuration.

- Filtering on TCP/UDP allows the user to specify port numbers as filtering criteria
- Select ICMP to allow/deny packets. Selecting ICMP allows to filter ICMP packets based on type and code

NOTE
The log option is functional only for router ACL's. The log option displays an informational logging message about the packet matching the entry sent to the console.

Permitting IP based traffic

The example below allows IP traffic from the source subnet to the destination subnet and denies all other traffic over an interface:

```
RFController(config-ext-nacl)#permit ip 192.168.1.10/24 192.168.2.0/24
rule-precedence 40
RFController(config-ext-nacl)#
```

Permitting Telnet based traffic

The example below permits Telnet traffic from the source subnet and the destination subnet and denies all other traffic over an interface:

```
RFController(config-ext-nacl)#permit tcp 192.168.4.0/24 192.168.5.0/24 eq 23
rule-precedence 10
RFController(config-ext-nacl)#
```

Permitting ICMP based traffic

The example below permits ICMP traffic and denies all other traffic over an interface:

```
RFController(config-ext-nacl)#permit icmp any any rule-precedence 30
RFController(config-ext-nacl)#)#
```

service

Extended ACL config commands

Invokes service commands to troubleshoot or debug the `(config-if) instance` configurations

Supported in the following platforms:

- Mobility RFS4000 Controller
- Mobility RFS6000 Controller
- Mobility RFS7000 Controller

Syntax

```
service show cli
```

Parameters

None

Example

```
RFController(config-ext-nacl)#service show cli
Extended ACL Config mode:
+-clrscr [clrscr]
+-deny
  +-icmp
    +-A.B.C.D/M
      +-A.B.C.D/M [(deny|permit|mark (8021p <0-7> | tos <0-255>)) (icmp)
(A.B.C.D/M | host A.B.C.D | any)(A.B.C.D/M | host A.B.C.D | any)(<0-255> |
<0-255> <0-255> |)(log|)(rule-precedence <1-5000> |)]
        +-<0-255> [(deny|permit|mark (8021p <0-7> | tos <0-255>)) (icmp)
(A.B.C.D/M | host A.B.C.D | any)(A.B.C.D/M | host A.B.C.D | any)(<0-255> |
<0-255> <0-255> |)(log|)(rule-precedence <1-5000> |)]
          +-<0-255> [(deny|permit|mark (8021p <0-7> | tos <0-255>)) (icmp)
(A.B.C.D/M | host A.B.C.D | any)(A.B.C.D/M | host A.B.C.D | any)(<0-255> |
<0-255> <0-255> |)(log|)(rule-precedence <1-5000> |)]
            +-log [(deny|permit|mark (8021p <0-7> | tos <0-255>)) (icmp)
(A.B.C.D/M | host A.B.C.D | any)(A.B.C.D/M | host A.B.C.D | any)(<0-255> |
<0-255> <0-255> |)(log|)(rule-precedence <1-5000> |)]
+-rule-precedence
.....................................................................................
.....................................................................................
.........................
RFController(config-ext-nacl)#
```

show

Extended ACL config commands

Displays current system information running on the controller

Supported in the following platforms:

- Mobility RFS4000 Controller
- Mobility RFS6000 Controller
- Mobility RFS7000 Controller

NOTE
The following commands display only for the Mobility RFS6000 Controller and the Mobility RFS4000 Controller:
- power
The following commands display only for the Mobility RFS7000 Controller and the Mobility RFS4000 Controller:
- port-channel
- static-channel-group

Syntax

```
show <paramater>
```

Parameters

?	Displays the parameters for which information can be viewed using the show command

Example

```
RFController(config-ext-nacl)#show ?
  access-list           Internet Protocol (IP)
  aclstats              Show ACL Statistics information
  alarm-log             Display all alarms currently in the system
  autoinstall           autoinstall configuration
  banner                Display Message of the Day Login banner
  boot                  Display boot configuration.
  clock                 Display system clock
  commands              Show command lists
  crypto                encryption module
  debugging             Debugging information outputs
  dhcp                  DHCP Server Configuration
  environment           show environmental information
  file                  Display filesystem information
  firewall              Wireless firewall
  ftp                   Display FTP Server configuration
  history               Display the session command history
  interfaces            Interface status
  ip                    Internet Protocol (IP)
  ldap                  LDAP server
  licenses              Show any installed licenses
  logging               Show logging configuration and buffer
  mac                   Internet Protocol (IP)
  mac-address-table     Display MAC address table
  mac-name              Displays the configured MAC names
```

```
  management             Display L3 Managment Interface name
  mobility               Display Mobility parameters
  ntp                    Network time protocol
  password-encryption    password encryption
  port-channel           Portchannel commands
  privilege              Show current privilege level
  radius                 RADIUS configuration commands
  redundancy             Display redundancy group parameters
  role                   Configure role parameters
  rtls                   Real Time Locating System commands
  running-config         Current Operating configuration
  securitymgr             Securitymgr parameters
  service-list           List of services
  sessions               Display current active open connections
  smtp-notifications     Display SNMP engine parameters
  snmp                   Display SNMP engine parameters
  snmp-server            Display SNMP engine parameters
  spanning-tree          Display spanning tree information
  startup-config         Contents of startup configuration
  static-channel-group   static channel group membership
  terminal               Display terminal configuration parameters
  timezone               Display timezone
  traffic-shape          Display traffic shaping
  upgrade-status         Display last image upgrade status
  users                  Display information about currently logged
                         in users
  version                Display software & hardware version
  virtual-ip             IP redundancy feature
  wireless               Wireless configuration commands
  wlan-acl               wlan based acl
  wwan                   Wireless wan interface
RFController(config-ext-nacl)#show
```

Configuring IP Extended ACL

IP Extended ACLs contain rules based on the following parameters:

- Source IP address
- Destination IP address
- IP Protocol
- Source Port–if protocol is TCP or UDP
- Destination Port–if protocol is TCP or UDP
- ICMP Type–if protocol is ICMP
- ICMP Code–if protocol is ICMP

  IP protocol, Source IP and Destination IP are mandatory parameters.You can create either a *Numbered IP Extended ACL* or a *Named IP Extended IP Address*.

  Execute the following commands to configure an IP Extended ACL:

1. To configure a numbered IP Extended ACL:

```
RFController(config)#access-list 2 deny ip host 1.2.3.4 any
rule-precedence 10
RFController(config)#access-list 2 permit tcp any host 2.3.4.5 eq 80
rule-precedence 20
RFController(config)#access-list 2 deny icmp any host 2.3.4.5
rule-precedence 30
```

2. To configure named IP Extended ACL:

```
RFController(config)#ip access-list extended ipextacl
RFController(config-ext-nacl)#deny ip host 1.2.3.4 any rule-precedence 10
RFController(config-ext-nacl)#permit tcp any host 2.3.4.5 eq 80
rule-precedence 20
RFController(config-ext-nacl)#deny icmp any host 2.3.4.5 rule-precedence
30
```

Chapter

Standard ACL Instance

15

In this chapter

The Standard ACL instance `(config-std-acl)` is used to manage the standard Access Control List entries associated with the controller.

To navigate to this instance, use the command:

```
RFController(config)#ip access-list standard [<ACL-name>|
       <1-99>|<1300-1999>]
RFController(config-std-acl)#
```

Standard ACL config commands

Table 15 summarizes the **`config-std-nacl`** commands:

TABLE 15 Standard ACL Config Command Summary

Command	Description	Ref.
clrscr	Clears the display screen	*page 472*
deny	Specifies packets to reject	*page 473*
end	Ends the current mode and moves to the EXEC mode	*page 475*
exit	Ends the current mode and moves to the previous mode	*page 476*
help	Displays the interactive help system	*page 477*
mark	Specifies packets to mark	*page 478*
no	Negates a command or sets its defaults	*page 480*
permit	Specifies packets to forward	*page 481*
service	Invokes service commands to troubleshoot or debug `(config-if)` instance configurations	*page 483*
show	Displays running system information	*page 484*

clrscr

Standard ACL config commands

Clears the display screen

Supported in the following platforms:

- Mobility RFS4000 Controller
- Mobility RFS6000 Controller
- Mobility RFS7000 Controller

Syntax

```
clrscr
```

Parameters

None

Example

```
RFController(config-std-nacl)#clrscr
RFController(config-std-nacl)#
```

deny

Standard ACL config commands

Specifies packets to reject

Supported in the following platforms:

- Mobility RFS4000 Controller
- Mobility RFS6000 Controller
- Mobility RFS7000 Controller

Syntax

```
deny [<source-IP/Mask>|any|host <IP>] {log} {rule-precedence
<1-5000>}
```

Parameters

[<source-IP/Mask>|any|host <IP>] *{log} {rule-precedence <1-5000>}*	Use with a deny command to reject packets • <source-IP/Mask>|any|host <IP> – The keyword <source-IP> is the source IP address of the network or host in dotted decimal format. The <Mask> is the network mask. For example, 10.1.1.10/24 indicates the first 24 bits of the source IP is used for matching. • any – any is an abbreviation for a source IP of 0.0.0.0 and source-mask bits equal to 0 • host – host is an abbreviation for the exact source <IP> (A.B.C.D format) and source-mask bits equal to 32 • log – Generates log messages when the packet coming from the interface matches an ACL entry. Log messages are generated only for router ACLs. • rule-precedence <1-5000> – Defines an integer value between 1-5000. This value sets the rule precedence in the ACL..

Usage Guidelines

Use this command to deny traffic based on the source IP address or network address. The last ACE in the access list is an implicit deny statement.

Whenever the interface receives the packet, its content is checked against all the ACEs in the ACL. It is allowed/denied based on the ACL configuration.

NOTE
The log option is functional only for router ACL's. The log option results in an informational logging message for the packet matching the entry sent to the console.

Example - denying traffic to the interface

The example below denies all traffic entering the interface (a log message is generated whenever the interface receives a packet):

```
RFController(config-std-nacl)#deny any log rule-precedence 50
RFController(config-std-nacl)#
```

Example - denying traffic only from source network

The example below denies traffic from the source network (xxx.xxx.1.0/24) and allows all other traffic to flow through the interface:

```
RFController(config-std-nacl)#deny xxx.xxx.1.0/24 rule-precedence 60
RFController(config-std-nacl)#permit any
```

end

Standard ACL config commands

Ends and exits from the current mode and moves to the PRIV EXEC mode. The prompt changes to `RFController#`

Supported in the following platforms:

- Mobility RFS4000 Controller
- Mobility RFS6000 Controller
- Mobility RFS7000 Controller

Syntax

```
end
```

Parameters

None

Example

```
RFController(config-std-nacl)#end
RFController#
```

exit

Standard ACL config commands

Ends the current mode and moves to previous mode (GLOBAL-CONFIG). The prompt changes to `RFController(config)#`

Supported in the following platforms:

- Mobility RFS4000 Controller
- Mobility RFS6000 Controller
- Mobility RFS7000 Controller

Syntax

```
exit
```

Parameters

None

Example

```
RFController(config-std-nacl)#exit
RFController(config)#
```

help

Standard ACL config commands

Displays the system's interactive help in HTML format

Supported in the following platforms:

- Mobility RFS4000 Controller
- Mobility RFS6000 Controller
- Mobility RFS7000 Controller

Syntax

```
help
```

Parameters

None

Example

```
RFController(config-std-nacl)#help
CLI provides advanced help feature.  When you need help,
anytime at the command line please press '?'.

If nothing matches, the help list will be empty and you must backup
until entering a '?' shows the available options.
Two styles of help are provided:
1. Full help is available when you are ready to enter a
   command argument (e.g. 'show ?') and describes each possible
   argument.
2. Partial help is provided when an abbreviated argument is entered
   and you want to know what arguments match the input
   (e.g. 'show ve?'.)

RFController(config-std-nacl)#
```

mark

Standard ACL config commands

Specifies packets to mark

Supported in the following platforms:

- Mobility RFS4000 Controller
- Mobility RFS6000 Controller
- Mobility RFS7000 Controller

Syntax

```
mark [8021p|dscp|tos]
mark 8021p <vlan-priority-value>
mark dscp <dscp-codepoint-value>
mark tos <tos-value> [<source-IP/Mask>|any|host <IP>] {log} {rule-precedence
<1-5000>}
```

Parameters

8021p <vlan-priority-value>	Sets the 802.1p VLAN user priority value to <vlan-priority-value> (0-7).
dscp <dscp-codepoint-value>	Sets the Differentiated Services Code Point code-point value to <dscp-codepoint-value> (0-63)
tos <tos-value>	Sets the TOS value to <tos-value>. The least significant two bits of the <tos-value> must be 0.
[<source-IP/Mask>| any|host <IP>] *{log} {rule-precedence <1-5000>}*	Use with a **mark** command to mark packets • <source-IP/Mask>|any|host <IP> – The keyword <source-IP> is the source IP address of the network or host in dotted decimal format. The <Mask> is the network mask. For example, 10.1.1.10/24 indicates the first 24 bits of the source IP is used for matching. • any – any is an abbreviation for a source IP of 0.0.0.0 and source-mask bits equal to 0 • host – host is an abbreviation for the exact source <IP> (A.B.C.D format) and source-mask bits equal to 32 • log – Optional.Generates log messages when the packet coming from the interface matches an ACL entry. Log messages are generated only for router ACLs. • rule-precedence <1-5000> – Optional. Defines an integer value between 1-5000. This value sets the rule precedence in the ACL.

Usage Guidelines

Use this command to mark traffic from the source network/host. Use the mark option to specify the t*ype of service* (TOS) and priority value. The TOS value is marked in the IP header. The 802.1p priority value is marked in the frame.

When the interface receives the packet, its content is checked against the ACEs in the ACL. It is marked based on the ACL configuration.

NOTE
The log option is functional only for router ACLs. The log option results in an informational logging message about the packet matching the entry sent to the console.

Marking tos for Source Network Traffic

The example below marks the *type of service* (TOS) value to 254 for all traffic coming from the source network:

```
RFController(config)#access-list 3 mark tos 254 xxx.xxx.3.0/24
RFController (config)#access-list 3 permit any
```

no

Standard ACL config commands

Negates a command or sets its defaults

Supported in the following platforms:

- Mobility RFS4000 Controller
- Mobility RFS6000 Controller
- Mobility RFS7000 Controller

Syntax

```
no [deny|mark|permit]
```

Negates all the syntax combinations used in deny, mark and permit designations.

Parameters

deny	Specifies packets to reject
mark	Specifies packets to mark
permit	Specifies packets to forward

Example

```
RFController(config-std-nacl)#no permit any rule-precedence 10
RFController(config-std-nacl)#

RFController(config-std-nacl)#no deny any rule-precedence 20
RFController(config-std-nacl)#

RFController(config-std-nacl)#no mark tos 4 192.168.2.0/24 rule-precedence 30
RFController(config-std-nacl)#
```

permit

Standard ACL config commands

Specifies packet to forward

Supported in the following platforms:

- Mobility RFS4000 Controller
- Mobility RFS6000 Controller
- Mobility RFS7000 Controller

Syntax

```
permit [<source-IP/Mask>|any|host <IP>] {log}
{rule-precedence <1-5000>}
```

Parameters

[<source-IP/Mask>| any|host <IP>] *{log} {rule-precedence <1-5000>}*	Use with a **permit** command to allow packets • <source-IP/Mask>|any|host <IP> – The keyword <source-IP> is the source IP address of the network or host in dotted decimal format. The <Mask> is the network mask. For example, 10.1.1.10/24 indicates the first 24 bits of the source IP is used for matching. • any – any is an abbreviation for a source IP of 0.0.0.0 and source-mask bits equal to 0 • host – host is an abbreviation for the exact source <IP> (A.B.C.D format) and source-mask bits equal to 32 • log – Generates log messages when the packet coming from the interface matches an ACL entry. Log messages are generated only for router ACLs. • rule-precedence <1-5000> – Defines an integer value between 1-5000. This value sets the rule precedence in the ACL.

Usage Guidelines

Use this command to allow traffic based on the source IP address or network address. The last ACE in the access list is an implicit deny statement.

```
Whenever the interface receives the packet, its content is checked against all
the ACEs in the ACL. It is allowed based on the ACL's configuration.
```

NOTE
The log option is functional only for router ACLs. The log option displays an informational logging message about the packet matching the entry sent to the console.

Example - permitting traffic to interface

The example below permits all the traffic that comes to the interface:

```
RFController(config-std-nacl)#permit any rule-precedence 50
RFController(config-std-nacl)#
```

Permitting Traffic from source network

The example below permits traffic from the source network and provides a log message:

```
RFController(config-std-nacl)#permit xxx.xxx.1.0/24 log rule-precedence 60
RFController(config-std-nacl)#
```

service

Standard ACL config commands

Invokes service commands to troubleshoot or debug `(config-if)` instance configurations

Supported in the following platforms:

- Mobility RFS4000 Controller
- Mobility RFS6000 Controller
- Mobility RFS7000 Controller

Syntax

```
service show cli
```

Parameters

cli	Displays the CLI tree of the current mode

Example

```
RFController(config-std-nacl)#service show cli
Standard ACL Config mode:
+-clrscr [clrscr]
+-deny
  +-A.B.C.D/M [(deny|permit|mark (8021p <0-7> | tos <0-255>))(A.B.C.D/M | host
A.B.C.D | any)(log|)(rule-precedence <1-5000> |)]
    +-log [(deny|permit|mark (8021p <0-7> | tos <0-255>))(A.B.C.D/M | host
A.B.C.D | any)(log|)(rule-precedence <1-5000> |)]
      +-rule-precedence
       +-<1-5000> [(deny|permit|mark (8021p <0-7> | tos <0-255>))(A.B.C.D/M |
host A.B.C.D | any)(log|)(rule-precedence <1-5000> |)]
    +-rule-precedence
      +-<1-5000> [(deny|permit|mark (8021p <0-7> | tos <0-255>))(A.B.C.D/M |
host A.B.C.D | any)(log|)(rule-precedence <1-5000> |)]
  +-any [(deny|permit|mark (8021p <0-7> | tos <0-255>))(A.B.C.D/M | host
A.B.C.D | any)(log|)(rule-precedence <1-5000> |)]
    +-log [(deny|permit|mark (8021p <0-7> | tos <0-255>))(A.B.C.D/M | host
A.B.C.D | any)(log|)(rule-precedence <1-5000> |)]
      +-rule-precedence
       +-<1-5000> [(deny|permit|mark (8021p <0-7> | tos <0-255>))(A.B.C.D/M |
host A.B.C.D | any)(log|)(rule-precedence <1-5000> |)]
    +-rule-precedence
      +-<1-5000> [(deny|permit|mark (8021p <0-7> | tos <0-255>))(A.B.C.D/M |
host A.B.C.D | any)(log|)(rule-precedence <1-5000> |)]
.....................................................................
.....................................................................
.........................................
RFController(config-std-nacl)#
```

show

Standard ACL config commands

Displays current system information running on the controller

Supported in the following platforms:

- Mobility RFS4000 Controller
- Mobility RFS6000 Controller
- Mobility RFS7000 Controller

NOTE
The following commands display only for the Mobility RFS6000 Controller and the Mobility RFS4000 Controller:
- power
The following commands display only for the Mobility RFS7000 Controller and the Mobility RFS4000 Controller:
- port-channel
- static-channel-group

Syntax

```
show <paramater>
```

Parameters

?	Displays all the parameters for which the information can be viewed using the show command

Example

```
RFController(config-std-nacl)#show ?
  access-list           Internet Protocol (IP)
  aclstats              Show ACL Statistics information
  alarm-log             Display all alarms currently in the system
  autoinstall           autoinstall configuration
  banner                Display Message of the Day Login banner
  boot                  Display boot configuration.
  clock                 Display system clock
  commands              Show command lists
  crypto                encryption module
  debugging             Debugging information outputs
  dhcp                  DHCP Server Configuration
  environment           show environmental information
  file                  Display filesystem information
  firewall              Wireless firewall
  ftp                   Display FTP Server configuration
  history               Display the session command history
  interfaces            Interface status
  ip                    Internet Protocol (IP)
  ldap                  LDAP server
  licenses              Show any installed licenses
  logging               Show logging configuration and buffer
  mac                   Internet Protocol (IP)
  mac-address-table     Display MAC address table
  mac-name              Displays the configured MAC names
  management            Display L3 Managment Interface name
```

```
  mobility              Display Mobility parameters
  ntp                   Network time protocol
  password-encryption   password encryption
  port                  Physical/Aggregate port interface
  port-channel          Portchannel commands
  privilege             Show current privilege level
  protocol-list         List of protocols
  radius                RADIUS configuration commands
  redundancy            Display redundancy group parameters
   rtls                  Real Time Locating System commands
  role                  Configure role parameters
  running-config        Current Operating configuration
  securitymgr           Securitymgr parameters
  service-list          List of services
  sessions              Display current active open connections
  smtp-notifications    Display the SNMP engine parameters
  snmp                  Display SNMP engine parameters
  snmp-server           Display SNMP engine parameters
  spanning-tree         Display spanning tree information
  startup-config        Contents of startup configuration
  static-channel-group  static channel group membership
  terminal              Display terminal configuration parameters
  timezone              Display timezone
  traffic-shape         Display traffic shaping
  upgrade-status        Display last image upgrade status
  users                 Display information about currently logged  in users
  version               Display software & hardware version
  virtual-IP            IP reduncancy feature
  wireless              Wireless configuration commands
  wlan-acl              wlan based acl
RFController(config-std-nacl)#show
```

Use case: configuring IP standard ACL

IP Standard ACLs contain rules based on *Source IP Address*. You can create either a *Numbered IP Standard ACL* or a *Named IP Standard IP Address*.

Execute the following CLI commands to configure an IP based standard ACL:

1. To configure numbered IP Standard ACL:

   ```
   RFController(config)#access-list 2 deny host 1.2.3.4 rule-precedence 10
   RFController(config)#access-list 3 deny host 1.2.3.4 rule-precedence 10
   RFController(config)#access-list 3 permit any rule-precedence 20
   ```

   Valid numbers for numbered IP Standard ACLs are from 1-99 and 1300-1999. In the above CLI example, ACL 3 denies host with IP 1.2.3.4 and allows all other hosts.

2. To configure an IP Standard ACL:

   ```
   RFController(config)#ip access-list standard ipst2
   RFController(config-std-nacl)#permit host 10.1.1.10 rule-precedence 30
   RFController(config-std-nacl)#deny any rule-precedence 20
   ```

Chapter

Extended MAC ACL Instance

16

In this chapter

Use the `(config-ext-macl)` instance to configure `mac access-list extended` ACLs. To navigate to this instance, use the command:

```
RFController(config)#mac access-list extended <acl-name>
RFController(config-ext-macl)#
```

MAC Extended ACL config commands

Table summarizes **`config-ext-macl`** commands:

TABLE 16 MAC Extended ACL Config Command Summary

Command	Description	Ref.
clrscr	Clears the display screen	*page 488*
deny	Specifies packets to reject	*page 489*
end	Ends the current mode and moves to the EXEC mode	*page 492*
exit	Ends the current mode and moves to the previous mode	*page 493*
help	Displays the interactive help system	*page 494*
mark	Specifies packets to mark	*page 495*
no	Negates a command or sets its defaults	*page 498*
permit	Specifies packets to forward	*page 499*
service	Invokes service commands to troubleshoot or debug the `(config-if)` instance configurations	*page 502*
show	Shows running system information	*page 504*

clrscr

MAC Extended ACL config commands

Clears the display screens

Supported in the following platforms:

- Mobility RFS4000 Controller
- Mobility RFS6000 Controller
- Mobility RFS7000 Controller

Syntax

```
clrscr
```

Parameters

None

Example

```
RFController(config-ext-macl)#clrscr
RFController(config-ext-macl)#
```

deny

MAC Extended ACL config commands

Specifies packets to reject

NOTE
Use a decimal value representation of ethertypes to implement a `permit/deny/mark` designation for a packet. The command set for Extended MAC ACLs provide the hexadecimal values for each listed ethertype. The controller supports all ethertypes. Use the decimal equivalent of the ethertype listed for any other ethertype.

Supported in the following platforms:

- Mobility RFS4000 Controller
- Mobility RFS6000 Controller
- Mobility RFS7000 Controller

Syntax

```
deny [<MAC/Mask>|any|host <MAC>] [<MAC/Mask>|any|
       host <MAC>] {[dot1p|rule-precedence|type|vlan]}

deny [<MAC/Mask>|any|host <MAC>] [<MAC/Mask>|any|
       host <MAC>] dot1p <0-7> {rule-precedence|type}

deny [<MAC/Mask>|any|host <MAC>] [<MAC/Mask>|any|
       host <MAC>] rule-precedence <1-5000>

deny [<MAC/Mask>|any|host <MAC>] [<MAC/Mask>|any|
       host <MAC>] type [8021p|<1-65535>|aarp|appletalk|apr|ip|
ipv6|ipx|rarp|wisp] {rule-precedence <precedence>}

deny [<MAC/Mask>|any|host <MAC>] [<MAC/Mask>|any|
       host <MAC>] vlan <1-4094> {rule-precedence|type}
```

Parameters

deny [<MAC/Mask>|any|host <MAC>] [<MAC/Mask>|any| host <MAC>] {[dot1p| rule-precedence|type|vlan]}	Define a source and destination MAC address and Mask specifying the bits to match. The source and destination wildcards can be any one of the following: • [<MAC/Mask>|any|host <MAC>]– Source MAC address and mask in the format xx:xx:xx:xx:xx:xx/xx:xx:xx:xx:xx:xx • any – Any source host • host – Exact source MAC address to match
dot1p <0-7>	Determine a 802.1p priority value to match. <priority> is in the range 0 to 7.
rule-precedence <1-5000>	Define an access-list entry precedence
type [8021q|<1-65535>| arp|appletalk|ip|ipv6|vlan|ipx|arp| wisp]	Set an ethertype value represented as an integer. Use keywords for well-known ethertypes (IP, IPv6, ARP etc.) • 8021q – VLAN Ether type (0*8100) • <1-65535> – Ether protocol number • aarp – AARP Ether Type (0*80F3) • appletalk – APPLETALK Ether Type (0*809B) • arp – ARP Ether Type (0*0806) • ip – IP Ether Type (0*0800) • ipv6 – IPv6 Ether Type (0*86DD) • ipx – IPX Ether Type (0*8137) • rarp – RARP Ether Type (0*8035) • wisp – WISP Ether Type (0*8783)
vlan<1-4095>	Set a VLAN tag ID to match

Usage Guidelines

The deny command disallows traffic based on layer 2 (data-link layer) data. The MAC access list denies traffic from a particular source MAC address or any MAC address. It can also disallow traffic from a list of MAC addresses based on the source mask.

The MAC access list can disallow traffic based on the VLAN and ethertype.

The most common ethertypes are:

- arp
- wisp
- ip
- 802.1q

NOTE
MAC ACL always takes precedence over IP based ACL's.

The last ACE in the access list is an implicit deny statement.

Whenever the interface receives the packet, its content is checked against all the ACEs in the ACL. It is allowed/denied based on the ACL configuration.

Example - denying traffic from any MAC address

The MAC ACL (in the example below) denies traffic from any source MAC address to a particular host MAC address:

```
RFController(config-ext-macl)#deny any host 00:01:ae:00:22:11
RFController(config-ext-macl)#
```

Example - denying dot1q tagged traffic

The MAC ACL (in the example below) denies dot1q tagged traffic from VLAN interface 5:

```
RFController(config-ext-macl)#deny any any vlan 5 type 8021q
RFController(config-ext-macl)#
```

Example - denying traffic between two MAC based hosts

The example below denies traffic between two hosts based on MAC addresses:

```
RFController(config-ext-macl)#deny host 01:02:fe:45:76:89 host
01:02:89:78:78:45
RFController(config-ext-macl)#
```

end

MAC Extended ACL config commands

Ends and exits the current mode and moves to the PRIV EXEC mode. The prompt changes to `RFController#`

Supported in the following platforms:

- Mobility RFS4000 Controller
- Mobility RFS6000 Controller
- Mobility RFS7000 Controller

Syntax

```
end
```

Parameters

None

Example

```
RFController(config-ext-macl)#end
RFController#
```

exit

MAC Extended ACL config commands

Ends the current mode and moves to the previous mode (GLOBAL-CONFIG). The prompt changes to `RFController(config)#`

Supported in the following platforms:

- Mobility RFS4000 Controller
- Mobility RFS6000 Controller
- Mobility RFS7000 Controller

Syntax

```
exit
```

Parameters

None

Example

```
RFController(config-ext-macl)#exit
RFController(config)#
```

help

MAC Extended ACL config commands

Displays the system's interactive help (in HTML format)

Supported in the following platforms:

- Mobility RFS4000 Controller
- Mobility RFS6000 Controller
- Mobility RFS7000 Controller

Syntax

```
help
```

Parameters

None

Example

```
RFController(config-ext-macl)#help
CLI provides advanced help feature.  When you need help,
anytime at the command line please press '?'.

If nothing matches, the help list will be empty and you must backup
until entering a '?' shows the available options.
Two styles of help are provided:
1. Full help is available when you are ready to enter a
   command argument (e.g. 'show ?') and describes each possible
   argument.
2. Partial help is provided when an abbreviated argument is entered
   and you want to know what arguments match the input
   (e.g. 'show ve?'.)

RFController(config-ext-macl)#
```

mark

MAC Extended ACL config commands

Specifies the packet to mark

NOTE
Use a decimal value representation of ethertypes to implement permit/deny/mark designations for a packet. An Extended MAC ACL provides the hexadecimal values for each listed ethertype. The controller supports all ethertypes. Use the decimal equivalent of the ethertype listed in the CLI or any other type of ethertype.

Supported in the following platforms:

- Mobility RFS4000 Controller
- Mobility RFS6000 Controller
- Mobility RFS7000 Controller

Syntax

```
mark [8021p|dscp|tos]
mark [8021p <vlan-priority-value>|dscp
<dscp-codepoint-value>|tos <tos-value>] [icmp|ip|tcp|udp]
mark [8021p <vlan-priority-value>|dscp
<dscp-codepointvalue>|tos <tos-value>] icmp [<source-IP/Mask>|any|host<IP>]
[<dest-IP/mask>|any|host <IP>]
{<ICMP-type> {<ICMPcode>}}
{log} {rule-precedence <1-5000>]}
mark [8021p <vlan-priority-value>|dscp
<dscp-codepointvalue>|tos <tos-value>] IP [<source-IP/mask>|any|host
<IP>][<dest-ip/mask>|any|host <IP>] {log} {rule-precedence <1-5000>}
mark [8021p <vlan-priority-value>|dscp
<dscp-codepointvalue>|tos <tos-value>] [tcp|udp]
[source-IP/Mask>|any|host<IP>] {eq <source-port>|range <starting-source-port>
<ending-source-port>} [<dest-IP/Mask|any|host <IP>] {eq <source-port>} {range
<starting-source-port> <ending-sourceport>}{log}
{rule-precedence <1-5000>}
```

Parameters

8021p<*0-7*>	Modifies the 802.1p VLAN user priority • xx:xx:xx:xx:xx:xx/xx:xx:xx:xx:xx:xx Source MAC address and mask • any – Any source host • host – Exact source MAC address to match
tos<*0-255*>	Modifies the TOS bits in an IP header • xx:xx:xx:xx:xx:xx/xx:xx:xx:xx:xx:xx Destination MAC address and mask • any – Any destination host • host – Exact destination MAC address to match
mark [<source-IP/Mask> |any|host<IP>]	Specifies the bits to match. The source wildcard can be any one of the following: • xx:xx:xx:xx:xx:xx/xx:xx:xx:xx:xx:xx Source MAC address and mask • any – Any source host • host – Exact source MAC address to match
mark [<dest-IP/mask>|any|host <IP>]	Specifies bits to match. The destination wildcard can be any one of the following: • xx:xx:xx:xx:xx:xx/xx:xx:xx:xx:xx:xx Destination MAC address and mask • any – Any destination host • host – Exact destination MAC address to match
dot1p<*0-7*>	Defines a VLAN 802.1p priority value to match
rule-precedence<*1-5000*>	Establishes an access-list entry precedence
type [8021q|<*1-65535*>| arp|appletalk|ip|ipv6ipx|rarp| vlan|wisp]	Defines an ethertype value represented as an integer or keyword for well-known ethertypes (such as: IP, IPv6, ARP)
vlan <*1-4095*>	Defines the VLAN tag ID to match
dscp <0-63>	Modify DSCP TOS bits in IP header • xx:xx:xx:xx:xx:xx/xx:xx:xx:xx:xx:xx Destination MAC address and mask • any – Any destination host • host – Exact destination MAC address to match

Usage Guidelines

Use the mark option to specify the t*ype of service* (tos) and priority value. The tos value is marked in the IP header and the 802.1p priority value is marked in the dot1q frame.

Whenever the interface receives the packet, its content is checked against all the ACEs in the ACL. It is marked based on the ACL's configuration.

Example - marking dot1p priority value for 802.1q tagged traffic

The example below marks the dot1p priority value to 6 for all 802.1q tagged traffic from VLAN interface 5:

```
RFController(config-ext-macl)#mark 8021p 6 any any vlan 5 type 8021q
RFController(config-ext-macl)#
```

Example - marking tos for IP traffic

The example below marks the tos field to 254 for IP traffic coming from the source MAC :

```
RFController(config-ext-macl)#mark tos 254 host 00:33:44:55:66:77 any type ip
RFController(config-ext-macl)#
```

no

MAC Extended ACL config commands

Negates a command or sets its defaults

Supported in the following platforms:

- Mobility RFS4000 Controller
- Mobility RFS6000 Controller
- Mobility RFS7000 Controller

Syntax

```
no [deny|mark|permit]
```

Negates all the syntax combinations used in deny, mark and permit designations to configure the Extended ACL

Parameters

deny	Specifies packets to reject
mark	Specifies packets to mark
permit	Specifies packets to forward

Example

```
RFController(config-ext-macl)#no mark tos 254 host 00:33:44:55:66:77 any type
ip rule-precedence 50
RFController(config-ext-macl)#

RFController(config-ext-macl)#no deny any any vlan 5 type 8021q
rule-precedence 10
RFController(config-ext-macl)#

RFController(config-ext-macl)#no permit any any type wisp rule-precedence 50
RFController(config-ext-macl)#
```

permit

MAC Extended ACL config commands

Specifies packets to forward

NOTE
Use a decimal value representation of ethertypes to implement permit/deny/mark designations for a packet. An Extended MAC ACL provides the hexadecimal values for each listed ethertype. The controller supports all ethertypes. Use the decimal equivalent of the ethertype listed in the CLI or any other type of ethertype.

Supported in the following platforms:

- Mobility RFS4000 Controller
- Mobility RFS6000 Controller
- Mobility RFS7000 Controller

Syntax

```
permit [icmp|ip|tcp|upd]
permit icmp [<source-IP/Mask>|any|host <IP>] [<dest-IP/
Mask>|any|host <IP>] {<ICMP-type> {<ICMP-code>}} {log}
{rule-precedence <1-5000>]}

permit ip [<source-IP/mask>|any|host <ip>] [<dest-IP/Mask>|any|host <ip>]
{log} {rule-precedence <1-5000>}

permit [tcp|udp] [<source-IP/Mask>|any|host <IP>] {eq
<source-port>|range <starting-source-port>
<ending-sourceport>}[<dest-IP/Mask|any|host <IP>] {eq <source-port>}{range
<starting-source-port>
<ending-source-port>} {log}{rule-precedence <1-5000>}
```

Parameters

permit [<source-IP/Mask>|any|host <IP>]	Specifies the bits to match. The source wildcard can be any one of the following: • **xx:xx:xx:xx:xx:xx/xx:xx:xx:xx:xx:xx** Source MAC address and mask • any – Uses any source host • host – Defines the MAC address to match
permit [<dest-IP/ Mask>|any|host <IP>] {<ICMP-type> {<ICMP-code>}}	Bit mask specifying the bits to match. The destination wildcard can be one of the following: • **xx:xx:xx:xx:xx:xx/xx:xx:xx:xx:xx:xx** Destination MAC address and mask • any – Uses any available destination host • host – Defines the destination MAC address
dot1p<*0-7*>	Establishes the 802.1p priority
rule-precedence<*1-5000*>	Defines an access list entry precedence
type(8021q|<*1-65535*>|aarp|arp|appletalk|ip|ipv6|ipx|rarp|vlan|wisp)	Sets an ethertype • 8021q **–VLAN Ether type (0*8100)** • <1-65535> **– Ether protocol number** • aarp **– AARP Ether Type (0*80F3)** • appletalk **– APPLETALK Ether Type (0*809B)** • arp **– ARP Ether Type (0*0806)** • ip **– IP Ether Type (0*0800)** • ipv6 **– IPv6 Ether Type (0*86DD)** • ipx **– IPX Ether Type (0*8137)** • rarp **– RARP Ether Type (0*8035)** • wisp **– WISP Ether Type (0*8783)**
vlan<*1-4095*>	Sets the VLAN ID

Usage Guidelines

When creating a Port ACL, the controller (by default) does not permit an ethertype WISP. Create a rule to allow WISP to adopt access points. Use the following command to adopt access points:

```
permit any any type wisp
```

NOTE
Use the following command to attach a MAC access list to a port on a layer 2 interface:
`mac access-group <acl number/name> in`

The permit command in the MAC ACL disallows traffic based on layer 2 (data-link layer) information. A MAC access list permits traffic from a source MAC address or any MAC address. It also has an option to allow traffic from a list of MAC addresses (based on the source mask).

The MAC access list can be configured to allow traffic based on VLAN information, ethernet type. Common types include:

- arp
- wisp
- ip
- 802.1q

The controller (by default) does not allow layer 2 traffic to pass through the interface. To adopt an access point through an interface, configure an access control list to allow an ethernet WISP. .v

NOTE
To apply an IP based ACL to an interface, a MAC access list entry to allow ARP is mandatory. A MAC ACL always takes precedence over IP based ACLs.

The last ACE in the access list is an implicit deny statement. Whenever the interface receives the packet, its content is checked against all the ACEs in the ACL. It is allowed/denied based on the ACL's configuration.

Example - permitting WISP traffic

The example below permits WISP traffic from any source MAC address to any destination MAC address:

```
RFController(config-ext-macl)#permit any any type wisp
RFController(config-ext-macl)#
```

Example - permitting ARP traffic

The example below permits arp based traffic from any source MAC address to any destination MAC address:

```
RFController(config-ext-macl)#permit any any type arp
RFController(config-ext-macl)#
```

Permitting IP traffic

The example below permits IP based traffic from a source MAC address to any destination MAC address:

```
RFController(config-ext-macl)#permit host 11:22:33:44:55:66 any type ip
RFController(config-ext-macl)#
```

service

MAC Extended ACL config commands

Invokes service commands to troubleshoot or debug `(config-if)` instance configurations

Supported in the following platforms:

- Mobility RFS4000 Controller
- Mobility RFS6000 Controller
- Mobility RFS7000 Controller

Syntax

```
service show cli
```

Parameters

show cli	Displays running system information

Example

```
RFController(config-ext-macl)#service show cli
MAC Extended ACL Config mode:
+-clrscr [clrscr]
+-deny
  +-XX:XX:XX:XX:XX:XX/XX:XX:XX:XX:XX:XX
    +-XX:XX:XX:XX:XX:XX/XX:XX:XX:XX:XX:XX [(deny|permit|mark (8021p <0-7> |
tos
<0-255>))(XX:XX:XX:XX:XX:XX/XX:XX:XX:XX:XX:XX | host XX:XX:XX:XX:XX:XX |
any)(XX
:XX:XX:XX:XX:XX/XX:XX:XX:XX:XX:XX | host XX:XX:XX:XX:XX:XX | any)(vlan
<1-4095>
| dot1p <0-7> |) (type (<1-65535> | ip | ipv6          | arp | wisp | 8021q | ra
rp | aarp | appletalk | ipx ) |)(rule-precedence <1-5000> |)]
      +-dot1p
        +-<0-7> [(deny|permit|mark (8021p <0-7> | tos
<0-255>))(XX:XX:XX:XX:XX:X
X/XX:XX:XX:XX:XX:XX | host XX:XX:XX:XX:XX:XX |
any)(XX:XX:XX:XX:XX:XX/XX:XX:XX:X
X:XX:XX | host XX:XX:XX:XX:XX:XX | any)(vlan <1-4095> | dot1p <0-7> |) (type
(<1
-65535> | ip | ipv6          | arp | wisp | 8021q | rarp | aarp | appletalk | ip
x ) |)(rule-precedence <1-5000> |)]
          +-rule-precedence
            +-<1-5000> [(deny|permit|mark (8021p <0-7> | tos
<0-255>))(XX:XX:XX:
XX:XX:XX/XX:XX:XX:XX:XX:XX | host XX:XX:XX:XX:XX:XX |
any)(XX:XX:XX:XX:XX:XX/XX:
XX:XX:XX:XX:XX | host XX:XX:XX:XX:XX:XX | any)(vlan <1-4095> | dot1p <0-7> |)
(t
ype (<1-65535> | ip | ipv6          | arp | wisp | 8021q | rarp | aarp | appleta
lk | ipx ) |)(rule-precedence <1-5000> |)]
          +-type
................................................................................
................................................................................
..............................................
```

```
RFController(config-ext-macl)#
```

show

MAC Extended ACL config commands

Displays current system information running on the controller

Supported in the following platforms:

- Mobility RFS4000 Controller
- Mobility RFS6000 Controller
- Mobility RFS7000 Controller

NOTE
The following commands display only for the Mobility RFS6000 Controller and the Mobility RFS4000 Controller:
- power
The following commands display only for the Mobility RFS7000 Controller and the Mobility RFS4000 Controller:
- port-channel
- static-channel-group

Syntax

```
show <paramater>
```

Parameters

?	Displays all the parameters for which information can be viewed using the show command

Usage Guidelines

The show access-list command displays the access lists configured for the controller. Provide the access list name or number to view specific ACL details

Example

```
RFController(config-ext-macl)#show ?
  access-list           Internet Protocol (IP)
  aclstats              Show ACL Statistics information
  alarm-log             Display all alarms currently in the system
  autoinstall           autoinstall configuration
  banner                Display Message of the Day Login banner
  boot                  Display boot configuration.
  clock                 Display system clock
  commands              Show command lists
  crypto                encryption module
  debugging             Debugging information outputs
  dhcp                  DHCP Server Configuration
  dpd                   wios dataplane
  environment           show environmental information
  file                  Display filesystem information
  firewall              Wireless firewall
  ftp                   Display FTP Server configuration
  history               Display the session command history
  interfaces            Interface status
  ip                    Internet Protocol (IP)
  ldap                  LDAP server
```

```
  licenses              Show any installed licenses
  logging               Show logging configuration and buffer
  mac                   Internet Protocol (IP)
  mac-address-table     Display MAC address table
  mac-name              Displays the configured MAC names
  management            Display L3 Managment Interface name
  mobility              Display Mobility parameters
  ntp                   Network time protocol
  password-encryption   password encryption
  port-channel          Portchannel commands
  protocol-list         List of protocols
  privilege             Show current privilege level
  radius                RADIUS configuration commands
  redundancy            Display redundancy group parameters
  rtls                  Real Time Locating System commands
  role                  Configure role parameters
  running-config        Current Operating configuration
  securitymgr           Securitymgr parameters
  service-list          List of services
  sessions              Display current active open connections
  mtp-notofication      Display SNMP engine parameters
  snmp                  Display SNMP engine parameters
  snmp-server           Display SNMP engine parameters
  spanning-tree         Display spanning tree information
  startup-config        Contents of startup configuration
  static-channel-group  static channel group membership
  terminal              Display terminal configuration parameters
  traffic-shape         Display traffic shaping
  timezone              Display timezone
  upgrade-status        Display last image upgrade status
  users                 Display information about currently logged in users
  version               Display software & hardware version
  virtual-ip            IP redundancy feature
  wireless              Wireless configuration commands
  wlan-acl              wlan based acl

RFController(config-ext-macl)#show
```

Configuring MAC Extended ACL

MAC Extended ACLs contain rules based on the following parameters:

- Source MAC address
- Destination MAC address
- Ethertype– accepts well known types like IP, ARP, VLAN or an integer value between 1-65535.
- VLAN-ID
- VLAN 802.1p user priority

Source and Destination MAC address are mandatory parameters.

Execute the following commands to configure a MAC extended ACL with different rule parameters on the controller:

```
RFController(config)#mac access-list extended macextacl
RFController(config-ext-macl)#permit 00:a0:f8:00:00:00 ff:ff:ff:00:00:00 any
rule-precedence 10
RFController(config-ext-macl)#deny any any type arp rule-precedence 20
RFController(config-ext-macl)#deny any any vlan 23 rule-precedence 30
```

Chapter

DHCP Server Instance

17

In this chapter

Use the `(config-dhcp)` instance to configure the DHCP server address pool associated with the controller.

To move to this instance, use the command.

```
RFController(config)#ip dhcp pool <pool-name>
RFController(config-dhcp)#
```

Also refer to Chapter 18, "DHCP Class Instance" for other DHCP related configurations.

DHCP Config commands

Table 17 summarizes **`config-dhcp`** commands:

TABLE 17 DHCP Config Commands

Command	Description	Ref.
address	Defines the DHCP server include range	*page 509*
bootfile	Assigns a boot file name. The bootfile name can contain letters, numbers, dots and hyphens. Consecutive dots and hyphens are not permitted	*page 510*
class	Associates a class with a pool and moves to the DHCP pool class configuration mode	*page 511*
client-identifier	Uses an ASCII string as a client identifier	*page 513*
client-name	Assigns a client name	*page 514*
clrscr	Clears the display screen	*page 515*
ddns	Configures *Dynamic DNS* (DDNS) values	*page 516*
default-router	Configures a default router's IP address	*page 517*
dns-server	Sets the IP address of a DNS Server	*page 518*
domain-name	Sets the domain name	*page 519*
end	Ends the current mode and moves to the EXEC mode	*page 520*
exit	Ends the current mode and moves to the previous mode	*page 521*
hardware-address	Defines the hardware address using either a dashed or dotted hexadecimal string	*page 522*
help	Displays the interactive help system in HTML format	*page 523*

TABLE 17 DHCP Config Commands

Command	Description	Ref.
host	Configures an IP address for the host	*page 524*
lease	Assigns the lease time for a DHCP leased IP address	*page 525*
netbios-name-server	Configures NetBIOS (WINS) name servers	*page 527*
netbios-node-type	Defines the NetBIOS node type	*page 528*
network	Sets a network number and mask for a DHCP Server	*page 529*
next-server	Configures the next server in boot process	*page 530*
no	Negates a command or sets its defaults	*page 531*
option	Assigns a name for a DHCP option	*page 532*
service	Invokes service commands to troubleshoot or debug `(config-dhcp)` instance configurations	*page 533*
show	Displays the running system information	*page 534*
unitcast-enable	Enables unicast for DHCP	*page 537*
update	Controls the usage of *Dynamic DNS* (DDNS)	*page 536*

address

DHCP Config commands

Specifies a range of addresses for the DHCP network pool

Supported in the following platforms:

- Mobility RFS4000 Controller
- Mobility RFS6000 Controller
- Mobility RFS7000 Controller

Syntax

```
address range <low IP address> <high IP address>
```

Parameters

range <low IP address> <high IP address>	Adds an address range for the DHCP server • low IP address – Defines the first IP address in the address range • high IP address – Defines the last IP address in the address range

Usage Guidelines

Use the `address` command to specify a range of addresses for the DHCP network pool. The DHCP server assigns IP address to DHCP clients from the address range. A high IP address is the upper limit for providing the IP address, and a low IP address is the lower limit for providing the IP address.

Use the `no address range` command to remove the DHCP address range.

Example

```
RFController(config-dhcp)#address range 2.2.2.2 2.2.2.50
RFController(config-dhcp)#
```

bootfile

DHCP Config commands

Assigns a bootfile name for the DHCP configuration on the network pool

Supported in the following platforms:

- Mobility RFS4000 Controller
- Mobility RFS6000 Controller
- Mobility RFS7000 Controller

Syntax

```
bootfile <FILE>
```

Parameters

bootfile <FILE>	Sets the boot image for BOOTP clients. The file name can contain letters, numbers, dots and hyphens. Consecutive dots and hyphens are not permitted.

Usage Guidelines

Use the `bootfile` command to specify the boot image. The boot file contains the boot image name used for booting the bootp clients (DHCP clients). Only one boot file is allowed per pool.

Use {`no} bootfile` command to remove the bootfile. Do not use the <file name> with the bootfile command as only one bootfile exists per pool. The command `[no] bootfile` removes the existing command from the pool.

Example

```
RFController(config-dhcp)#bootfile bootexample.txt
RFController(config-dhcp)#
```

class

DHCP Config commands

Associates a DHCP class with a pool

This command is used in Step 4 of *Creating a DHCP User Class*.

The CLI prompt moves to a sub-instance `(config-dhcp-class)`.The configuration mode changes from `(config-dhcp)# class` to `(config-dhcp-class)`.
Refer to *config-dhcp-class on page 512* for a `(config-dhcp-class)` command summary.

Supported in the following platforms:

- Mobility RFS4000 Controller
- Mobility RFS6000 Controller
- Mobility RFS7000 Controller

Syntax

```
class <class-name>
```

Parameters

class <class -name>	Associates a class with a pool and enters the DHCP pool class configuration mode

Example

```
RFController(config-dhcp)#class RFControllerDHCPclass
RFController(config-dhcpclass)#
```

Creating a DHCP User Class

Follow the steps below to create a DHCP User Class:

1. Create a DHCP class named **`RFControllerDHCPclass`**. The controller supports a maximum of 32 DHCP classes.

   ```
   RFController(config)#ip dhcp class RFControllerDHCPclass
   RFController(config-dhcpclass)#
   ```

2. Create a USER class named **`MC800`**. The mode changes to `(config-dhcpclass)`. The controller supports a maximum of 8 users classes per DHCP class.

   ```
   RFController(config-dhcpclass)#option user-class MC800
   RFController(config-dhcpclass)#
   ```

3. Create a Pool named **`WID`**, using `(config)#` mode.

   ```
   RFController(config)#ip dhcp pool WID
   RFController(config-dhcp)#
   ```

4. Associate the DHCP class, created in Step 1 with the pool created in Step 3. The controller supports the association of 8 DHCP classes with a pool.

   ```
   RFController(config-dhcp)#class RFControllerDHCPclass
   RFController(config-dhcp-class)#
   ```

5. The controller moves to a new mode (config-dhcp-class). Use this mode to add an address range used for the DHCP class associated with the pool.

```
RFController(config-dhcp-class)#address range 11.22.33.44
```

config-dhcp-class

Use `(config-dhcp)# class` to enter the (**`config-dhcp-class) instance`**. Use this instance to set an address range for a DHCP user class within a DHCP server address pool.

Table 18 summarizes **`config-dhcp-class`** commands.

TABLE 18 config-dhcp-class commands

Command	*Description*
address	Sets an address range for a DHCP class in a DHCP server address pool
clrscr	Clears the display screen
end	Ends the current mode and moves to the EXEC mode
exit	Ends the current mode and moves to the previous mode
help	Displays the interactive help system in HTML format
no	Negates a command or sets its defaults
service	Assists in troubleshooting or debugging issues
show	Displays running system information

address

config-dhcp-class

Sets an address range for a DHCP class within a DHCP server address pool

Syntax

```
address range <low IP Address> <high IP Address>
```

Parameters

range <low IP Address> <high IP Address>	Assigns an address range for the DHCP class • <low IP Address> – Defines the low IP address • <high IP Address> – Defines the high IP address

Example

```
RFController(config-dhcp-class)#address range 11.22.13.14 11.22.33.56
RFController(config-dhcp-class)#
```

client-identifier

DHCP Config commands

Assigns a name to the client-identifier

A client identifier is used to reserve an IP address for a DHCP client.

Supported in the following platforms:

- Mobility RFS4000 Controller
- Mobility RFS6000 Controller
- Mobility RFS7000 Controller

Syntax

```
client-identifier <identifier>
```

Parameters

client-identifier <identifier>	Prepends a null character. Use \\0 at the beginning (a single \ in the input is ignored)

Example

```
RFController(config-dhcp)#client-identifier testid
RFController(config-dhcp)#
```

client-name

DHCP Config commands

Adds name for DHCP clients

Supported in the following platforms:

- Mobility RFS4000 Controller
- Mobility RFS6000 Controller
- Mobility RFS7000 Controller

Syntax

```
client-name <name>
```

Parameters

client-name <name>	Use `client-name` to add a client name (the domain name must not be included)

Example

```
RFController(config-dhcp)#client-name testpc
RFController(config-dhcp)#
```

clrscr

DHCP Config commands

Clears the display screen

Supported in the following platforms:

- Mobility RFS4000 Controller
- Mobility RFS6000 Controller
- Mobility RFS7000 Controller

Syntax

```
clrscr
```

Parameters

None

Example

```
RFController(config-dhcp)#clrscr
RFController(config-dhcp)#
```

ddns

DHCP Config commands

Sets dynamic DNS parameters

Supported in the following platforms:

- Mobility RFS4000 Controller
- Mobility RFS6000 Controller
- Mobility RFS7000 Controller

Syntax

```
ddns [domainname|multiple-user-class|server|ttl]

ddns domainname <name>
ddns multiple-user-class
ddns server <IP Address>
ddns ttl <1-864000>
```

Parameters

domainname <name>	Sets the domain name used for DDNS updates
multiple-user-class	Enables the multiple user class option
server <IP >	Specifies the server to which DDNS updates have been sent • <IP> – Defines an IP address in dotted decimal format
ttl <1-864000>	Sets a *Time To Live* (TTL) value for DDNS updates • <1-864000> – TTL value in seconds

Usage Guidelines

Use `update dns override` to enable an internal DHCP server to send DDNS updates for resource records (RRs) A, TXT and PTR. A DHCP server can always override the client even if the client is configured to perform the updates.

In the DHCP server network pool, FQDN is defined as the DDNS domain name. This is used internally in DHCP packets between the DHCP server on the controller and the DNS server.

Example

```
RFController(config-dhcp)#ddns domainname TestDomain.com
RFController(config-dhcp)#

RFController(config-dhcp)#ddns multiple-user-class
RFController(config-dhcp)#

RFController(config-dhcp)#ddns ttl 1000
RFController(config-dhcp)#
```

default-router

DHCP Config commands

Configures the default router or gateway IP address for the network pool. To remove the default router list, use the `no default-router` command.

Supported in the following platforms:

- Mobility RFS4000 Controller
- Mobility RFS6000 Controller
- Mobility RFS7000 Controller

Syntax

```
default-router <IP>
```

Parameters

default-router < IP>	Specifies the default router IP address for the network pool • < IP> – Sets the router's IP address

Usage Guidelines

The IP address of the router should be on the same subnet as the client subnet.

Example

```
RFController(config-dhcp)#default-router 2.2.2.1
RFController(config-dhcp)#
```

dns-server

DHCP Config commands

Sets the DNS server's IP address available to all DHCP clients connected to the pool. Use the `no dns-server` command to remove the DNS server list.

Supported in the following platforms:

- Mobility RFS4000 Controller
- Mobility RFS6000 Controller
- Mobility RFS7000 Controller

Syntax

```
dns-server <IP address>
```

Parameters

dns-server <IP address>	Configures the DNS server's IP address • <IP address> – Sets the server's IP address. Up to 8 IPs can be set.

Usage Guidelines

For DHCP clients, the DNS server's IP address maps the host name to an IP address. DHCP clients use the DNS server's IP address based on the order (sequence) configured.

Example

```
RFController(config-dhcp)#dns-server 2.2.2.222
RFController(config-dhcp)#
```

domain-name

DHCP Config commands

Sets the domain name for the network pool. Use the `no domain-name` command to remove the domain name.

Supported in the following platforms:

- Mobility RFS4000 Controller
- Mobility RFS6000 Controller
- Mobility RFS7000 Controller

Syntax

```
domain-name <name>
```

Parameters

domain-name <name>	Defines the domain name for the network pool

Usage Guidelines

The domain name cannot exceed 256 characters.

Example

```
RFController(config-dhcp)#domain-name Engineering
RFController(config-dhcp)#
```

end

DHCP Config commands

Exits the current mode and moves to the PRIV EXEC mode. The prompt changes to `RFController#`

Supported in the following platforms:

- Mobility RFS4000 Controller
- Mobility RFS6000 Controller
- Mobility RFS7000 Controller

Syntax

```
end
```

Parameters

None

Example

```
RFController(config-dhcp)#end
RFController#
```

exit

DHCP Config commands

Ends the current mode and moves to the previous mode (GLOBAL-CONFIG). The prompt changes to `RFController#(config)#`

Supported in the following platforms:

- Mobility RFS4000 Controller
- Mobility RFS6000 Controller
- Mobility RFS7000 Controller

Syntax

```
exit
```

Parameters

None

Example

```
RFController(config)#ip dhcp pool TestPool
RFController(config-dhcp)#exit
RFController(config)#
```

hardware-address

DHCP Config commands

Reserves an IP address (manually) based on a DHCP client's hardware address. Use the `no hardware-address` command to remove this from the DHCP pool.

Supported in the following platforms:

- Mobility RFS4000 Controller
- Mobility RFS6000 Controller
- Mobility RFS7000 Controller

Syntax

```
hardware-address <MAC> {[ethernet|token-ring]}
```

Parameters

hardware-address
<MAC> {ethernet|token-ring}
	Sets the client's hardware address to <MAC>. <MAC> can be in the format xx-xx-xx-xx-xx-xx (dashed hexadecimal string) or XX:XX:XX:XX:XX:XX (dotted hexadecimal string)
	• <MAC> {ethernet|token-ring} – Defines a dashed hexadecimal string
	• <MAC> {ethernet|token-ring} – Sets a dotted hexadecimal string.
	  • ethernet – Ethernet
	  • token-ring – Token ring network

Usage Guidelines

Accepts only hexadecimal values

Example

```
RFController(config-dhcp)#hardware-address 00:01:23:45:32:22
RFController(config-dhcp)#
```

help

DHCP Config commands

Displays the system's interactive help in HTML format

Supported in the following platforms:

- Mobility RFS4000 Controller
- Mobility RFS6000 Controller
- Mobility RFS7000 Controller

Syntax

```
help
```

Parameters

None

Example

```
RFController(config-dhcp)#help
CLI provides advanced help feature.  When you need help,
anytime at the command line please press '?'.

If nothing matches, the help list will be empty and you must backup
until entering a '?' shows the available options.
Two styles of help are provided:
1. Full help is available when you are ready to enter a
   command argument (e.g. 'show ?') and describes each possible
   argument.
2. Partial help is provided when an abbreviated argument is entered
   and you want to know what arguments match the input
   (e.g. 'show ve?'.)

RFController(config-dhcp)#
```

host

DHCP Config commands

Defines a fixed IP address for the host in dotted decimal format

Use the `no host` command to remove the host from the DHCP pool.

Supported in the following platforms:

- Mobility RFS4000 Controller
- Mobility RFS6000 Controller
- Mobility RFS7000 Controller

Syntax

```
host <IP>
```

Parameters

host <IP>	Sets a fixed address for the host • <IP > – Sets an IP address in dotted decimal format

Usage Guidelines

The DHCP host pool (used to manually assign an IP address based on hardware address/client identifier) configuration must contain a host IP address, client name and hardware address/client identifier.

The host IP address must belong to a subnet on the controller. There must be a DHCP network pool corresponding to that host IP address. There is no limit to the number of manual bindings. However, you can configure only one manual binding per host pool.

Example

```
RFController(config-dhcp)#host 2.2.2.111
RFController(config-dhcp)#
```

lease

DHCP Config commands

Sets a valid lease time for the IP address used by DHCP clients in the network pool

Supported in the following platforms:

- Mobility RFS4000 Controller
- Mobility RFS6000 Controller
- Mobility RFS7000 Controller

Syntax

```
lease [{<0-365> <0-23> <0-59>}|infinite]
```

Parameters

lease [{<0-365> <0-23> <0-59>} |infinite]	Sets the lease time for an IP address
	• <0-365> –Sets the lease period in days. Days can be made as 0 only when hours and/or mins are greater than 0.
	  • <0-23> – Sets the hours for the lease period. Hours can be 0 only when days and/or minutes are configured with a value greater than 0.
	  • <0-59> – Sets the minutes for the lease period. Minutes can be 0 only when days and/or hours are configured with a value greater than 0.
	• infinite – Sets the lease period as infinite.

Usage Guidelines

If lease parameter is not configured on the DHCP network pool, the default value is used. The default value of the lease is 24 hours.

The lease value for DHCP host pool is infinite. Hence the lease configuration is not applicable for DHCP host pool

NOTE
The factory default lease period for a pool – network pool or host pool is configured as 1 day.

Example

```
RFController(config-dhcp)#lease 1 0 0
RFController(config-dhcp)#

RFController(config)#show running-config
.....................................
.....................................
.....................................
ip dhcp pool Test4lease
 host 3.33.33.3
 client-name test4lease
 client-identifier tested4lease
.....................................
.....................................
RFController(config)#
```

```
RFController(config)#show running-config include-factory
.....................................
ip dhcp pool Test4lease
 lease 1 0 0
 no domain-name
 no bootfile
 no dns-server
 no default-router
 no next-server
 no netbios-name-server
 no netbios-node-type
 no unicast-enable
 no update dns
 no ddns domainname
 no ddns ttl
 no ddns multiple-user-class
 host 3.33.33.3
 client-name test4lease
 client-identifier tested4lease
 no hardware-address
.....................................
RFController(config)#
```

netbios-name-server

DHCP Config commands

Sets the netbios-name server's IP address

Supported in the following platforms:

- Mobility RFS4000 Controller
- Mobility RFS6000 Controller
- Mobility RFS7000 Controller

Syntax

```
netbios-name-server <IP>
```

Parameters

netbios-name-server <IP>	Defines the NetBIOS (WINS) name server • <IP > – Sets the NetBIOS name server's IP address

Example

```
RFController(config-dhcp)#netbios-name-server 2.2.2.222
RFController(config-dhcp)#
```

netbios-node-type

DHCP Config commands

Defines the netbios-node type

Supported in the following platforms:

- Mobility RFS4000 Controller
- Mobility RFS6000 Controller
- Mobility RFS7000 Controller

Syntax

```
netbios-node-type [b-node|h-node|m-node|p-node]
```

Parameters

netbios-node-type [b-node | h-node | m-node | p-node]	Defines the NetBIOS (WINS) name servers • b-node – Broadcast node • h-node – Hybrid node • m-node – Mixed node • p-node – Peer-to-peer node

Example

```
RFController(config-dhcp)#netbios-node-type p-node
RFController(config-dhcp)#
```

network

DHCP Config commands

Sets the network pool's IP address

This address maps the current DHCP pool with a specific network.

Supported in the following platforms:

- Mobility RFS4000 Controller
- Mobility RFS6000 Controller
- Mobility RFS7000 Controller

Syntax

```
network [<IP>|<IP/Mask>]
```

Parameters

network [<IP>|<IP/Mask>]	Sets the network number and mask • <IP> – Network number in dotted decimal format • <IP/Mask> – Network number and mask

Usage Guidelines

Ensure a VLAN interface (with specific network/subnet) exists on the controller before mapping a DHCP pool to a particular network.

Example

```
RFController(config-dhcp)#network  2.2.2.0/24
RFController(config-dhcp)#
```

next-server

DHCP Config commands

Sets the IP address of the next server in the boot process

Supported in the following platforms:

- Mobility RFS4000 Controller
- Mobility RFS6000 Controller
- Mobility RFS7000 Controller

Syntax

```
next-server <IP>
```

Parameters

next-server <IP>	Sets the next server in boot process • <IP> – Defines the server's IP address

Example

```
RFController(config-dhcp)#next-server 2.2.2.22
RFController(config-dhcp)#
```

no

DHCP Config commands

Negates a command or sets its defaults

Supported in the following platforms:

- Mobility RFS4000 Controller
- Mobility RFS6000 Controller
- Mobility RFS7000 Controller

Syntax

```
no [address|bootfile|class|client-identifier|client-name|
ddns|default-router|dns-server|domain-name|hardware-address|
host|lease|netbios-name-server|netbios-node-type|network|
next-server|option|update|unicast-table]
```

Parameters

The `no` command negates any command associated with it. Wherever required, use the same parameters associated with the command getting negated.

Example

```
RFController(config)#no ip dhcp pool hotpool
RFController(config)#

RFController(config)#no ip dhcp pool test
RFController(config)#

RFController(config-dhcp)#no update dns
RFController(config-dhcp)#
```

option

DHCP Config commands

Defines the DHCP option used in DHCP pools

Supported in the following platforms:

- Mobility RFS4000 Controller
- Mobility RFS6000 Controller
- Mobility RFS7000 Controller

Syntax

```
option <option-name> [<IP>|<option-name>]
```

Parameters

option name [<IP>| <option-name>]	Sets raw DHCP options
	• <option-name> – Sets the name of the DHCP option
	  • <IP> – Sets the IP value of the DHCP option
	  • <option-name> – Sets the ASCII value of the DHCP option

Usage Guidelines

Defines non standard DHCP option codes (0-254)

NOTE
An option name in ASCII format accepts backslash (\) as an input but is not displayed in the output (Use `show runnig config` to view the output). Use double backslash to represent a single backslash.

Example

```
RFController(config)#ip dhcp option option189 189 ascii
RFController(config)#
```

service

DHCP Config commands

Invokes service commands to troubleshoot or debug `(config-dhcp)` instance configurations

Supported in the following platforms:

- Mobility RFS4000 Controller
- Mobility RFS6000 Controller
- Mobility RFS7000 Controller

Syntax

```
service show cli
```

Parameters

show cli	Displays the CLI tree of the current mode

Example

```
RFController(config-dhcp)#service show cli
DHCP Server Config mode:
+-address
  +-range
    +-A.B.C.D [address range A.B.C.D ( A.B.C.D |)]
      +-A.B.C.D [address range A.B.C.D ( A.B.C.D |)]
+-bootfile
  +-WORD [bootfile WORD]
+-class
  +-WORD [class WORD]
+-client-identifier
  +-WORD [client-identifier WORD]
+-client-name
  +-WORD [client-name WORD]
+-clrscr [clrscr]
+-ddns
  +-domainname
    +-WORD [ddns domainname WORD]
  +-multiple-user-class [ddns multiple-user-class]
  +-server
    +-A.B.C.D [ddns server A.B.C.D (A.B.C.D|)]
.........................
.....................................................
RFController(config-dhcp)#
```

show

DHCP Config commands

Displays current system information

Supported in the following platforms:

- Mobility RFS4000 Controller
- Mobility RFS6000 Controller
- Mobility RFS7000 Controller

NOTE
The following commands display only for the Mobility RFS6000 Controller and the Mobility RFS4000 Controller:
- power
The following commands display only for the Mobility RFS7000 Controller and the Mobility RFS4000 Controller:
- port-channel
- static-channel-group

Syntax

```
show <paramater>
```

Parameters

?	Displays parameters for which information can be viewed using the show command

Example

```
RFController(config-dhcp)#show ?
  access-list           Internet Protocol (IP)
  aclstats              Show ACL Statistics information
  alarm-log             Display all alarms currently in the system
  autoinstall           autoinstall configuration
  banner                Display Message of the Day Login banner
  boot                  Display boot configuration.
  clock                 Display system clock
  commands              Show command lists
  crypto                encryption module
  debugging             Debugging information outputs
  dhcp                  DHCP Server Configuration
  environment           show environmental information
  file                  Display filesystem information
  firewall              Wireless firewall
  ftp                   Display FTP Server configuration
  history               Display the session command history
  interfaces            Interface status
  ip                    Internet Protocol (IP)
  ldap                  LDAP server
  licenses              Show any installed licenses
  logging               Show logging configuration and buffer
  mac                   Internet Protocol (IP)
  mac-address-table     Display MAC address table
  mac-name              Displays the configured mac names
  management            Display L3 Managment Interface name
```

```
  mobility              Display Mobility parameters
  ntp                   Network time protocol
  password-encryption   password encryption
  port                  Physical/Aggregate port interface
  port-channel          Portchannel commands
  privilege             Show current privilege level
  protocol-list         List of protocols
  radius                RADIUS configuration commands
  redundancy            Display redundancy group parameters
  rtls                  Real Time Locating System commands
  role                  Configure role parameters
  running-config        Current Operating configuration
  securitymgr           Securitymgr parameters
  service-list          List of services
  sessions              Display current active open connections
  smtp-notification     Display SNMP engine parameters
  snmp                  Display SNMP engine parameters
  snmp-server           Display SNMP engine parameters
  spanning-tree         Display spanning tree information
  startup-config        Contents of startup configuration
  static-channel-group  static channel group membership
  terminal              Display terminal configuration parameters
  timezone              Display timezone
  traffic-shape         Display traffic shaping
  upgrade-status        Display last image upgrade status
  users                 Display information about currently logged
                        in users
  version               Display software & hardware version
  virtual-ip            IP redundancy list
  wireless              Wireless configuration commands
  wlan-acl              wlan based acl

RFController(config-dhcp)#
```

update

DHCP Config commands

Controls the usage of the DDNS service

Supported in the following platforms:

- Mobility RFS4000 Controller
- Mobility RFS6000 Controller
- Mobility RFS7000 Controller

Syntax

```
update dns override
```

Parameters

update dns override	Controls the usage of the DDNS service • dns override – Dynamic DNS Configuration • override – Enable Dynamic Updates by onboard DHCP Server

Usage Guidelines

A DHCP client cannot perform updates for RR's A, TXT and PTR. Use `update (dns) (override)` to enable the internal DHCP Server to send DDNS updates for resource records (RR's) A, TXT and PTR. The DHCP Server can override the client, even if the client is configured to perform the updates.

In the network pool of DHCP Server, FQDN is configured as the DDNS domain name. This is used internally in DHCP packets between the controllers DHCP Server and the DNS server.

Example

```
RFController(config-dhcp)#update dns override
RFController(config-dhcp)#
```

unitcast-enable

DHCP Config commands

Enables unicast for DHCP offer and DHCP Ack

Supported in the following platforms:

- Mobility RFS4000 Controller
- Mobility RFS6000 Controller
- Mobility RFS7000 Controller

Syntax

```
unicast-enable
```

Parameters

```
None
```

Example

```
RFController(config-dhcp)#unicast-enable
RFController(config-dhcp)#
```

Configuring the DHCP server using controller CLI

The controller DHCP configuration is conducted by creating pools and mapping them to L3 interfaces (SVI).

- A Network pool is the pool with “include” ranges. When the network pool is mapped to a L3 interface, DHCP clients requesting IPs from the L3 interface get an IP from the configured range.
- A host pool is the pool used to assign static/fixed IP address to DHCP clients.

Creating network pool

To create a network pool:

1. Create a DHCP server dynamic address pool.

   ```
   RFController(config)#ip dhcp pool test
   ```

2. Map the DHCP pool to the network pool.

   ```
   RFController(config-dhcp)#network 192.168.0.0/24
   ```

3. Add the address range for the dynamic pool.

   ```
   RFController(config-dhcp)#address range 192.168.0.30 192.168.0.60
   ```

4. Assign a domain name (as appropriate) to this dynamic pool.

   ```
   RFController(config-dhcp)#domain-name test.com
   ```

5. Configure the DNS server's IP address.

   ```
   RFController(config-dhcp)#dns-server 192.168.0.10 192.168.0.11
   ```

6. Configure the DHCP client's IP address lease period.

   ```
   RFController(config-dhcp)#lease 10
   ```

7. Exit from the DHCP instance upon creation of the network pool.

   ```
   RFController(config-dhcp)#exit
   ```

8. Start the DHCP server to initiate the network pool.

   ```
   RFController(config)#service dhcp
   ```

Creating a Host Pool

To create a host pool:

1. Create a DHCP server host address pool.

   ```
   RFController(config)#ip dhcp pool hostpool
   ```

2. Assign the client name of the host for which static allocation is required.

   ```
   RFController(config-dhcp)#client-name linuxbox
   ```

3. Assign an IP address for the host.

   ```
   RFController(config-dhcp)#host 192.168.0.50
   ```

4. Configure the hardware address of the host.

   ```
   RFController(config-dhcp)#hardware 00:a0:f8:6f:6b:88
   ```

5. Exit from the DHCP instance upon creation of the network pool.

   ```
   RFController(config-dhcp)#exit
   ```

6. Start the DHCP Server to instantiate the network pool.

   ```
   RFController(config)#service dhcp
   ```

Troubleshooting DHCP Configuration

1. The DHCP Server is disabled by default. Use the following command to enable the DHCP Server:

   ```
   RFController(config)#service dhcp
   ```

   This command administratively enables the DHCP server. If the DHCP configuration is incomplete, it is possible the DHCP server will be disabled even after the execution of this command.

2. Use the **network** command to map the network pool to interface.

   ```
   network 192.168.0.0/24
   ```

   In the above example, 192.168.0.0/24 represents the L3 interface. When you execute this command, no check is performed to endorse whether an interface (with the specified IP/Netmask) exists. The verification is not performed because you can create a pool and map it to non existing L3 interface.

   When you add a L3 interface and assign an IP address to it, the DHCP server gets enabled/started on this interface. If you have a pool for network 192.168.0.0/24, but the L3 interface is 192.168.0.0/16, DHCP is not enabled on 192.168.0.0/16, since it is different from 192.168.0.0/24.

3. A network pool without any include range is as good as not having a pool. Add a include range using the **address range** command.

   ```
   address range 192.168.0.30 192.168.0.30
   ```

4. To work properly, a host pool should have the following 3 items configured:

   - client-name (CLI is **client-name <name>**)
   - fixed-address CLI is **host <ip>**)
   - hardware-address/client-identifier

   The hardware address is **hardware-address <addr>**

   The client-identifier is **client-identifier <id>**

   If you use **client-identifier** instead of **hardware-address**, a DHCP client sends the client-identifier when it requests for IP address. The Client - identifier has to be configured in the DHCP Client as an ASCII value and the same has to be used in the DHCP server option (for example, the Client- identifier option).

5. A host pool should have its corresponding network pool configured, otherwise the host pool is useless. The fixed IP address configured in the host pool must be in the subnet of the corresponding network pool.

6. If you create a pool and map it to an interface, it automatically gets enabled, provided DHCP is enabled at a global level. Use the **no network** command to disable DHCP on a per pool/interface basis.

7. To set a newly created pool as a network pool, use one of the following commands:

   - network (for example, network 192.168.0.0/24)
   - address range (for example, address range 192.168.0.30 192.168.0.50)

8. To set a newly created pool as a host pool, use one of the following commands:

   - host (for example, host 192.168.0.1)

- client-name (For example, client-name "MailUsers")
- client-identifier (For example, client-identifier "aabb:ccdd")
- hardware-address (For example, hardware-address “aa:bb:cc:dd:ee:ff”)

9. A pool can be configured either as the host pool or network pool, but not both.
10. A host pool can have either **client-identifier** or **hardware-address** configured, but not both.
11. An excluded address range has a higher precedence than an included address range. Thus, if a range is part of both an excluded and included range, it will be excluded.
12. DHCP options are first defined at the global level using **ip dhcp option <name> <code> <type>**. The value for these options are defined using the **option** under the DHCP pool context.

Creating a DHCP Option

To create a DHCP option:

1. To create a non standard option named “tftp-server”.

   ```
   RFController(config)#ip dhcp option tftp-server 183 ip
   ```

2. Enter the DHCP pool —”test”.

   ```
   RFController(config)#ip dhcp pool test
   ```

3. Assign a value to the DHCP option configured above.

   ```
   RFController(config-dhcp)#option tftp-server 192.168.0.100
   ```

4. Exit the DHCP instance.

   ```
   RFController(config-dhcp)#exit
   ```

Chapter

DHCP Class Instance

18

In this chapter

Use the (config-dhcpclass) instance to configure DHCP user classes. The controller supports a maximum of 8 user classes per DHCP class. To navigate to this instance use the command:

```
RFController(config)#ip dhcp class <class-name>
RFController(config-dhcpclass)#
```

Refer to *ip on page 412* and *DHCP Config commands on page 507* for other DHCP related configurations.

DHCP Server Class config commands

Table 19 summarizes `config-std-nacl` commands:

TABLE 19 DHCP Server Class Config Commands

Command	Description	Ref.
clrscr	Clears the display screen	*page 544*
end	Ends the current mode and moves to the EXEC mode	*page 545*
exit	Ends the current mode and moves to the previous mode	*page 546*
help	Displays the interactive help system in HTML format	*page 547*
multiple-user-class	Enables multiple user class options	*page 548*
no	Negates a command or sets its defaults	*page 549*
option	Defines DHCP Server options	*page 550*
service	Invokes service commands to troubleshoot or debug `(config-if)` instance configurations	*page 551*
show	Displays running system information	*page 552*

clrscr

DHCP Server Class config commands

Clears the display screen

Supported in the following platforms:

- Mobility RFS4000 Controller
- Mobility RFS6000 Controller
- Mobility RFS7000 Controller

Syntax

```
clrscr
```

Parameters

None

Example

```
RFController(config-dhcpclass)#clrscr
RFController(config-dhcpclass)#
```

end

DHCP Server Class config commands

Ends and exits the current mode and moves to the PRIV EXEC mode. The prompt changes to `RFController#`

Supported in the following platforms:

- Mobility RFS4000 Controller
- Mobility RFS6000 Controller
- Mobility RFS7000 Controller

Syntax

```
end
```

Parameters

None

Example

```
RFController(config-dhcpclass)#end
RFController#
```

exit

DHCP Server Class config commands

Ends the current mode and moves to the previous mode (GLOBAL-CONFIG). The prompt changes to `RFController(config)#`

Supported in the following platforms:

- Mobility RFS4000 Controller
- Mobility RFS6000 Controller
- Mobility RFS7000 Controller

Syntax

```
exit
```

Parameters

None

Example

```
RFController(config-dhcpclass)#exit
RFController(config)#
```

help

DHCP Server Class config commands

Displays the system's interactive help in HTML format

Supported in the following platforms:

- Mobility RFS4000 Controller
- Mobility RFS6000 Controller
- Mobility RFS7000 Controller

Syntax

```
help
```

Parameters

None

Example

```
RFController(config-dhcpclass)#help
CLI provides advanced help feature.  When you need help,
anytime at the command line please press '?'.

If nothing matches, the help list will be empty and you must backup
until entering a '?' shows the available options.
Two styles of help are provided:
1. Full help is available when you are ready to enter a
   command argument (e.g. 'show ?') and describes each possible
   argument.
2. Partial help is provided when an abbreviated argument is entered
   and you want to know what arguments match the input
   (e.g. 'show ve?'.)

RFController(config-dhcpclass)#
```

multiple-user-class

DHCP Server Class config commands

Enables the multiple-user-class option

Supported in the following platforms:

- Mobility RFS4000 Controller
- Mobility RFS6000 Controller
- Mobility RFS7000 Controller

Syntax

```
multiple-user-class
```

Parameters

None

Example

```
RFController(config-dhcpclass)#multiple-user-class
RFController(config-dhcpclass)#
```

no

DHCP Server Class config commands

Negates a command or sets its defaults

Supported in the following platforms:

- Mobility RFS4000 Controller
- Mobility RFS6000 Controller
- Mobility RFS7000 Controller

Syntax

```
no [multiple-user-class|option]
np option user-class <class-name>
```

Parameters

multiple-user-class	Disables the multiple user class option
option user-class <class-name>	Modifies the parameters of existing DHCP server options • user-class <class-name> – Configures DHCP-Server user class options • <class-name> – ASCII value of user-class option

Example

```
RFController(config-dhcpclass)#no multiple-user-class
RFController(config-dhcpclass)#
```

option

DHCP Server Class config commands

Specifies a value for DHCP user class options

Supported in the following platforms:

- Mobility RFS4000 Controller
- Mobility RFS6000 Controller
- Mobility RFS7000 Controller

Syntax

```
option user-class <class-name>
```

Parameters

user-class <class-name>	Creates/modifies DHCP server user class options • <class-name> – ASCII value of user-class option

Example

```
RFController(config-dhcpclass)#option user-class MC800
RFController(config-dhcpclass)#
```

Creating a DHCP user class

Complete the steps below to create a DHCP user class:

5. Create a DHCP class named *RFControllerDHCPclass*. The controller supports a maximum of 32 DHCP classes.

```
RFController(config)#ip dhcp class RFControllerDHCPclass
RFController(config-dhcpclass)#
```

6. Create a USER class named **MC800**. The privilege mode changes to `(config-dhcpclass)`. The controller supports a maximum of 8 user classes per DHCP class.

```
RFController(config-dhcpclass)#option user-class MC800
RFController(config-dhcpclass)#
```

7. Create a Pool named **WID**, using the `(config)#` mode.

```
RFController(config)#ip dhcp pool WID
RFController(config-dhcp)#
```

8. Associate the DHCP class, created in Step 1 with the pool created in Step 3. The controller supports the association of 8 DHCP classes with a pool.

```
RFController(config-dhcp)#class RFControllerDHCPclass
RFController(config-dhcp-class)#
```

9. The controller moves to a new mode (config-dhcp-class). Use this mode to add an address range for the DHCP class associated with the pool.

```
RFController(config-dhcp-class)#address range 11.22.33.44
```

service

DHCP Server Class config commands

Invokes service commands to troubleshoot or debug `(config-if)` instance configurations

Supported in the following platforms:

- Mobility RFS4000 Controller
- Mobility RFS6000 Controller
- Mobility RFS7000 Controller

Syntax

```
service show cli
```

Parameters

None

Example

```
RFController(config-dhcpclass)#service show cli
DHCP Server Class Config mode:
+-clrscr [clrscr]
+-do
  +-LINE [do LINE]
+-end [end]
+-exit [exit]
+-help [help]
+-multiple-user-class [multiple-user-class_cmd]
+-no
  +-multiple-user-class [no multiple-user-class_cmd]
  +-option
    +-user-class
      +-WORD [no option user-class WORD]
+-option
  +-user-class
    +-WORD [option user-class WORD]
+-quit [quit]
+-s
  +-commands [show commands]
    +-WORD [show commands WORD]
  +-running-config [show running-config]
    +-full [show running-config full]
.................................................................
.................................................................RFControll
er(config-dhcpclass)#
```

show

DHCP Server Class config commands

Displays current system information

Supported in the following platforms:

- Mobility RFS4000 Controller
- Mobility RFS6000 Controller
- Mobility RFS7000 Controller

NOTE
The following commands display only for the Mobility RFS6000 Controller and the Mobility RFS4000 Controller
- power
The following commands display only for the Mobility RFS7000 Controller and the Mobility RFS4000 Controller:
- port-channel
- static-channel-group

Syntax

```
show <parameters>
```

Parameters

?	Displays the parameters for which information can be viewed using the show command

Example

```
RFController(config-dhcpclass)#show ?
  access-list           Internet Protocol (IP)
  aclstats              Show ACL Statistics information
  alarm-log             Display all alarms currently in the system
  autoinstall           autoinstall configuration
  banner                Display Message of the Day Login banner
  boot                  Display boot configuration.
  clock                 Display system clock
  commands              Show command lists
  crypto                encryption module
  debugging             Debugging information outputs
  dhcp                  DHCP Server Configuration
  environment           show environmental information
  file                  Display filesystem information
  firewall              Wireless firewall
  ftp                   Display FTP Server configuration
  history               Display the session command history
  interfaces            Interface status
  ip                    Internet Protocol (IP)
  ldap                  LDAP server
  licenses              Show any installed licenses
  logging               Show logging configuration and buffer
  mac                   Internet Protocol (IP)
  mac-address-table     Display MAC address table
  mac-name              Displays the configured mac names
  management            Display L3 Managment Interface name
```

```
  mobility              Display Mobility parameters
  ntp                   Network time protocol
  password-encryption   password encryption
  port                  Physical/Aggregate port interface
  port-channel          Portchannel commands
  privilege             Show current privilege level
  protocol-list         List of protocols
  radius                RADIUS configuration commands
  redundancy            Display redundancy group parameters
  rtls                  Real Time Locating System commands
  role                  Configure role parameters
  running-config        Current Operating configuration
  securitymgr           Securitymgr parameters
  service-list          List of services
  sessions              Display current active open connections
  smtp-notification     Display SNMP engine parameters
  snmp                  Display SNMP engine parameters
  snmp-server           Display SNMP engine parameters
  spanning-tree         Display spanning tree information
  startup-config        Contents of startup configuration
  static-channel-group  static channel group membership
  terminal              Display terminal configuration parameters
  timezone              Display timezone
  traffic-shape         Display traffic shaping
  upgrade-status        Display last image upgrade status
  users                 Display information about currently logged
                        in users
  version               Display software & hardware version
  virtual-ip            IP redundancy list
  wireless              Wireless configuration commands
  wlan-acl              wlan based acl

RFController(config-dhcpclass)#show

RFController(config-dhcpclass)#show ip dhcp binding
IP               MAC/Client-Id       Expiry Time
--               -------------       -----------
RFController(config-dhcpclass)#

RFController(config-dhcpclass)#show ip dhcp class RFControllerDHCPclass
!
ip dhcp class DHCPclass
 option user-class MC800
RFController(config-dhcpclass)#


RFController(config-dhcpclass)#show ip dhcp pool WID
!
ip dhcp pool WID
 class RFControllerDHCPclass
  address range 11.22.33.44
RFController(config-dhcpclass)#
```

Chapter

Radius Server Instance

19

In this chapter

Use the `(config-radsrv)` instance to configure local RADIUS server parameters. Local (Onboard) RADIUS server commands are listed under this mode. To navigate to this instance, use the command:

```
RFController(config)#radius-server local
RFController(config-radsrv)#
```

Radius configuration commands

Table 20 summarizes the Radius server configuration command:

TABLE 20 RADIUS Server Command Summary

Command	Description	Ref.
authentication	Configures the authentication scheme used with the RADIUS server	*page 557*
ca	Defines CA parameters	*page 558*
clrscr	Clears the display screen	*page 559*
crl-check	Enables a *Certificate Revocation List* (CRL) check	*page 560*
end	Ends the current mode and moves to the EXEC mode	*page 561*
exit	Ends the current mode and moves to the previous mode	*page 562*
group	Sets RADIUS user group parameters. **NOTE:** This command navigates to another sub-instance called **`config-radsrv-group`** with its own command summary. v	*page 563*
help	Displays the interactive help system	*page 573*
ldap-server	Sets LDAP server parameters	*page 574*
nas	Sets RADIUS client parameters	*page 577*
no	Negates a command or sets its defaults	*page 578*
proxy	Defines the RADIUS proxy server configuration	*page 579*
rad-user	Sets the RADIUS user configuration	*page 580*
server	Configures server certificate parameters	*page 583*
service	Invokes service commands to troubleshoot or debug **`(config-radsrv)`** instance configurations	*page 584*

TABLE 20 RADIUS Server Command Summary

Command	Description	Ref.
show	Displays running system information	*page 585*
ldap-group-verification	Sets LDAP Group Verification	*page 587*

authentication

Radius configuration commands

Configures the authentication scheme used with the RADIUS server

Supported in the following platforms:

- Mobility RFS4000 Controller
- Mobility RFS6000 Controller
- Mobility RFS7000 Controller

Syntax

```
authentication [data-source|eap-auth-type]
authentication data-source [ldap|local]
authentication eap-auth-type [all|peap-gtc|
peap-mschapv2|tls|ttls-md5|ttls-mschapv2|ttls-pap]
```

Parameters

authentication
data-source [ldap|local]
	Configures authentication
	• data-source [ldap|local] – Sets the RADIUS data source for user authentication
	  • ldap - Remote LDAP Server
	  • local - Local user database

eap-auth-type [all| peap-gtc| peap-mschapv2|tls| ttls-md5|ttls-mschapv2 ttls-pap]	Defines RADIUS EAP and default authentication configurations • all – Enables TTLS and PEAP settings • peap-gtc – Defines the EAP and PEAP settings used with the default authentication configuration • peap-mschapv2 – Sets the EAP/PEAP type used with mschapv2 • tls – Defines an EAP/TLS configuration scheme • ttls-md5 – Sets the EAP/TTLS configuration used with the default md5 authentication scheme • ttls-mschapv2 – Sets the EAP/TTLS configuration used with the default mschapv2 authentication scheme • ttls-pap – Sets the EAP/TTLS configuration used with the default pap authentication scheme

Usage Guidelines

Set **`eap-auth-type`** to **`all`** to service RADIUS requests received from wireless clients. Setting `eap-auth-type` to `peap-gtc/peap-mschapv2` ensures `peap-gtc/peap-mschapv2` service only.

Similarly, setting `eap-auth-type` to `ttls-md5/ttls-mschapv2/ttls-pap` services all ttls authentication requests from wireless clients.

Setting `eap-auth-type` to `tls` ensures only tls authentication is serviced.

Example

```
RFController(config-radsrv)#authentication eap-auth-type peap-mschapv2
RFController(config-radsrv)#

RFController(config-radsrv)#authentication data-source ldap
RFController(config-radsrv)#
```

ca

Radius configuration commands

Configures CA (*Certificate Authority*) parameters

Supported in the following platforms:

- Mobility RFS4000 Controller
- Mobility RFS6000 Controller
- Mobility RFS7000 Controller

Syntax

```
ca trust-point <trustpoint-name>
```

Parameters

trust-point <trustpoint-name>	Defines the trustpoint configuration • <trustpoint-name> – Displays the existing trustpoint name

Usage Guidelines

Configures the trustpoint used by the local RADIUS server. Create the **`trustpoint`** before it can be used by the **`crypto pki trustpoint`** command.

The default trust point in use is – `default-trustpoint`.

Example

```
RFController(config)#radius-server local
RFController(config-radsrv)#ca trust-point tp1
RFController(config-radsrv)#
```

clrscr

Radius configuration commands

Clears the display screen

Supported in the following platforms:

- Mobility RFS4000 Controller
- Mobility RFS6000 Controller
- Mobility RFS7000 Controller

Syntax

```
clrscr
```

Parameters

None

Example

```
RFController(config-radsrv)#clrscr
RFController(config-radsrv)#
```

crl-check

Radius configuration commands

Enables a *Certificate Revocation List* (CRL) check

To enable the certificate revocation list, ensure the `crl list` is loaded using a `crypto pki import <trustpoint-name> crl` command.

Supported in the following platforms:

- Mobility RFS4000 Controller
- Mobility RFS6000 Controller
- Mobility RFS7000 Controller

Syntax

```
crl-check enable
```

Parameters

enable	Enables the CRL check

Usage Guidelines

TLS uses certificates for authentication. CRL (updated with a trustpoint), contains index numbers of revoked certificates. The CRL checks for any revoked certificates used for `tls` authentication.

Example

```
RFController(config-radsrv)#crl-check enable
RFController(config-radsrv)#
```

end

Radius configuration commands

Ends and exits the current mode and moves to the PRIV EXEC mode. The prompt changes to `RFController#`

Supported in the following platforms:

- Mobility RFS4000 Controller
- Mobility RFS6000 Controller
- Mobility RFS7000 Controller

Syntax

```
end
```

Parameters

None

Example

```
RFController(config-radsrv)#end
RFController#
```

exit

Radius configuration commands

Ends the current mode and moves to the previous mode (GLOBAL-CONFIG). The prompt changes to `RFController(config)#`

Supported in the following platforms:

- Mobility RFS4000 Controller
- Mobility RFS6000 Controller
- Mobility RFS7000 Controller

Syntax

```
exit
```

Parameters

None

Example

```
RFController(config-radsrv)#exit
RFController(config)#
```

group

Radius configuration commands

Configures RADIUS user groups

The CLI moves to the `config-radsrv-group` sub-instance to create a new group.

The prompt changes from `RFController(config-radsrv)#` to `RFController(config-radsrv-group)#`

Supported in the following platforms:

- Mobility RFS4000 Controller
- Mobility RFS6000 Controller
- Mobility RFS7000 Controller

Table 21 summarizes the RADIUS user group commands within the **`(config-radsrv-group)`** sub-instance.

TABLE 21 RADIUS User Group Command Summary

Command	Description	Ref.
clrscr	Clears the display screen	*page 563*
end	Ends the current mode and moves to the EXEC mode	*page 564*
exit	Ends the current mode and moves to the previous mode	*page 564*
group	Sets RADIUS user group parameters	*page 564*
guest-group	Defines guest group permissions	*page 565*
help	Displays the interactive help system in HTML format	*page 565*
no	Negates a command or sets its defaults	*page 566*
policy	Defines the RADIUS group access policy configuration	*page 566*
rad-user	Adds a RADIUS user to this group	*page 568*
rate-limit	Sets rate limit for group	*page 568*
service	Invokes RADIUS service commands if stopped	*page 569*
show	Displays running system information	*page 569*

clrscr

group

Clears the display screen

Syntax

```
clrscr
```

Parameters

None

Example

```
RFController(config-radsrv-group)#clrscr
RFController(config-radsrv-group)#
```

end

group

Ends and exits the current mode and changes to the PRIV EXEC mode. The prompt changes to **RFController#**

Syntax

```
end
```

Parameters

None

Example

```
RFController(config-radsrv-group)#end
RFController#
```

exit

group

Ends the current mode and moves to the previous mode (`config-radsrv`). The prompt changes to **RFController(config)#**.

Syntax

```
exit
```

Parameters

None

Example

```
RFController(config-radsrv-group)#exit
RFController(config-radsrv)#group
```

group

group

Establishes RADIUS user group parameters. This command creates a group within the existing RADIUS group

Syntax

```
group <group-name>
```

Parameters

<group-name>	Defines the RADIUS group name

Example

```
RFController(config-radsrv-group)#group TestGroup
RFController(config-radsrv-group)#
```

guest-group

group

Manages a guest user linked with a hotspot. Create a guest-user and associate it with the guest-group. The guest-user and the policies of the guest group are used for hotspot authentication/authorization.

Syntax

```
guest-group enable
```

Parameters

guest-group enable	Defines this group as a guest group

Usage Guidelines

Creates a guest group. The guest user created using `rad-user` can only be part of the guest group.

Example

```
RFController(config-radsrv-group)#guest-group enable
RFController(config-radsrv-group)#
```

help

group

Displays the system's interactive help in HTML format.

Syntax

```
help
```

Parameters

None

Example

```
RFController(config-radsrv-group)#help
CLI provides advanced help feature. When you need help,
anytime at the command line please press '?'.

If nothing matches, the help list will be empty and you must backup
until entering a '?' shows the available options.
Two styles of help are provided:
1. Full help is available when you are ready to enter a
   command argument (e.g. 'show ?') and describes each possible
   argument.
2. Partial help is provided when an abbreviated argument is entered
   and you want to know what arguments match the input
   (e.g. 'show ve?'.)

RFController(config-radsrv-group)#
```

no

group

Use this command to negate a command or set its defaults

Syntax

```
no [policy|rad-user|rate-limit]
no policy [day|time|vlan|wlan]
no policy wlan [<1-256>|all] <1-256>
no rate-limit [wired-to-wireless|wireless-to-wired]
```

Parameters

policy [day|time|vlan|wlan]	Defines the RADIUS group access policy configuration
	• day – Resets the access policy (days of permitted access) for this group
	• time – Configures the group's hourly access permissions
	• vlan – Sets the VLAN ID for the group
	• wlan [<1-256>|all] – Configures WLAN access policy for this group
	  • <1-256> – Sets the WLAN range for the access policy
	  • all – Removes all the WLAN allowed

rad-user [<name>|all]	Removes a user from this group • <name> – Defines an existing user name in this group • all – Removes all users from this group
rate-limit [wired-to-wireless|wireless-to-wired]	Negate a command or set its defaults • wired-to-wireless –uplink direction - from wireless client to network • wireless-to-wired – down-link-direction - from network to wireless client

Example

```
RFController(config-radsrv-group)#no policy day
RFController(config-radsrv-group)#

RFController(config-radsrv-group)#no policy time
RFController(config-radsrv-group)#

RFController(config-radsrv-group)#no policy vlan
RFController(config-radsrv-group)#

RFController(config-radsrv-group)#no policy wlan 2 5
RFController(config-radsrv-group)#

RFController(config-radsrv-group)#no rad-user all
RFController(config-radsrv-group)#

RFController(config-radsrv-group)#no service radius
%%Info: Radius service stopped...
RFController(config-radsrv-group)#
```

policy

group

Sets the authorization policies for a particular group (like day/time of access, WLANs allowed etc.).

NOTE
A user-based VLAN is effective only if dynamic VLAN authorization is enabled for the WLAN (as defined within the WLAN Configuration screen).

Syntax

```
policy [day|time|vlan|wlan]
policy day [all|su|mo|tu|we|th|fr|sa|weekdays]
policy time [start <0-23> <0-59>] [end <0-23> <0-59>]
policy vlan <1-4094>
```

Parameters

day [all|su|mo|tu|we|th|fr|sa|weekdays]	Day of access policy configuration • all – All days (from Sunday to Saturday) • su – Sunday • mo – Monday • tu – Tuesday • we – Wednesday • th – Thursday • fr – Friday • sa – Saturday • weekdays – Allows access only during weekdays (M-F)
time [start <0-23> <0-59>] [end <0-23> <0-59>]	Sets the access policy time for this group • start – Sets the start time • end – Defines the end time (must be greater than the start time) • <0-23> – Sets the hourly (hh) access limit • <0-59> – Sets the minute (mm) access limit
vlan <1-4096>	Sets the VLAN ID for this group • <1-4096> – Defines the VLAN range
wlan <1-256>	Sets the WLAN access policy for this group • <1-256> – Sets the WLAN index

Example

```
RFController(config-radsrv-group)#policy day weekdays
RFController(config-radsrv-group)#

RFController(config-radsrv-group)#policy time start 12 12 end 22 22
RFController(config-radsrv-group)#

RFController(config-radsrv-group)#policy vlan 20
RFController(config-radsrv-group)#

RFController(config-radsrv-group)#policy wlan 20 21 22 23
RFController(config-radsrv-group)#
```

rad-user

Radius configuration commands

Adds an existing RADIUS user to this group. If the RADIUS user is not available in the Onboard RADIUS server's database, create a new RADIUS user using the `rad-user` command from within the `(config-radsrv)` mode.
For more information, see *rad-user on page 580*.

NOTE
It is strictly recommended to set hotspot simultaneous-users to 1 for corresponding WLAN as guest user is being assigned access-duration.

Syntax

```
rad-user <name>
```

Parameters

<name>	Existing RADIUS user name

Example

```
RFController(config-radsrv)#rad-user user1 password user1
RFController(config-radsrv)#group group1
RFController(config-radsrv-group)#rad-user user1
RFController(config-radsrv-group)#
```

rate-limit

Radius configuration commands

Sets the rate limit for the RADIUS Server group

Syntax

```
rate-limit [wired-to-wireless|wireless-to-wired ]
<100-100000>
```

Parameters

wired-to-wireless <100-100000>	Down link direction from network to wireless client • <100-100000> – Rate in the range of <100-100000> kbps
wireless-to-wired <100-100000>	Up link direction from wireless client to network • <100-100000> – Rate in the range of <100-100000> kbps

Usage Guidelines

Use `[no] rate-limit [wired-to-wireless|wireless-to-wired]`to remove the rate limit applied to the group.

`[no] rate-limit [wireless-to-wired]` sets the rate limit back to unlimited

Example

```
RFController(config-radsrv-group)#rate-limit wired-to-wireless 100
RFController(config-radsrv-group)#

RFController(config-radsrv-group)#rate-limit wireless-to-wired 1000
```

```
RFController(config-radsrv-group)#
```

service

Radius configuration commands

Invokes RADIUS service commands (if they have been stopped). This command enables the RADIUS server. A RADIUS restart is executed only from the `config` mode.

Syntax

```
service show cli
```

Parameters

None

Example

```
RFController(config-radsrv-group)#service show cli
Radius user group configuration mode:
+-clrscr [clrscr]
+-do
  +-LINE [do LINE]
+-end [end]
+-exit [exit]
+-group
  +-WORD [group WORD]
+-guest-group
  +-enable [guest-group enable]
+-help [help]
.....................................................................
.....................................................................
.........................................
RFController(config-radsrv-group)#
```

show

Radius configuration commands

Displays current system information running on the controller

Syntax

```
show <paramater>
```

Parameters

?	Displays the parameters for which information can be viewed using the show command

Example

```
RFController(config-radsrv-group)#show ?
  aap-wlan-acl          wlan based acl
  aap-wlan-acl-stats    IP filtering wlan based statistics
  access-list           Internet Protocol (IP)
  aclstats              Show ACL Statistics information
  alarm-log             Display all alarms currently in the system
```

```
  arpi                  ARPI Configuration
  autoinstall           autoinstall configuration
  banner                Display Message of the Day Login banner
  boot                  Display boot configuration.
  clock                 Display system clock
  commands              Show command lists
  crypto                encryption module
  debugging             Debugging information outputs
  dhcp                  DHCP Server Configuration
  environment           show environmental information
  espi                  ESPI Configuration
  file                  Display filesystem information
  firewall              Wireless firwall
  ftp                   Display FTP Server configuration
  history               Display the session command history
  interfaces            Interface status
  ip                    Internet Protocol (IP)
  ldap                  LDAP server
  licenses              Show any installed licenses
  logging               Show logging configuration and buffer
  mac                   Internet Protocol (IP)
  mac-name              Displays the co nfigured MAC names
  mac-address-table     Display MAC address table
  management            Display L3 Managment Interface name
  mobility              Display Mobility parameters
  ntp                   Network time protocol
  password-encryption   password encryption
  power                 show power over ethernet command
  privilege             Show current privilege level
  radius                RADIUS configuration commands
  redundancy            Display redundancy group parameters
  redundancy-history    Display state transition history of
  role                  Configure role parameters
  securitymgr           Securitymgr parameters
  sessions              Display current active open connections
  smtp-notifications    Display SNMP engine parameters
  snmp                  Display SNMP engine parameters
  snmp-server           Display SNMP engine parameters
  sole                  Smart Opportunistic Location Engine
                        Configuration
  spanning-tree         Display spanning tree information
  startup-config        Contents of startup configuration
  tags                  Tags/Assets (passive, active, wi-fi, uwb)
                        Information
  static-channel-group  Display static channel group membership
  terminal              Display terminal configuration parameters
  timezone              Display timezone
  traffic-shape         Display traffic shaping
  upgrade-status        Display last image upgrade status
  users                 Display information about currently logged
                        in users
  version               Display software & hardware version
  virtual-ip            IP redundancy feature
  wireless              Wireless configuration commands
  wlan-acl              wlan based acl

RFController(config-radsrv-group)#
```

Example–creating a group

The **(config-radsrv-group)** sub-instance is explained in the example below:

1. Create a group called Sales in the local RADIUS server database.
   RFController(config-radsrv)#group sales
2. Check the RADIUS user group's configuration.

   RFController(config-radsrv-group)#?

   RADIUS user group configuration commands:
3. Use a **policy** command to configure group policies for the group created in Step 1.
   ```
   RFController(config-radsrv-group)#policy ?
   day   Day of access policy configuration
   time  Configure time of access policy for this group
   vlan  VLAN id for this group
   wlan  Configure wlan access policy for this group

   RFController(config-radsrv-group)#policy day weekdays
   RFController(config-radsrv-group)#policy time start 12 30 end 15 30
   ```
4. Use the **policy vlan** command to assign a VLAN ID of 10 to the Sales group.
   RFController(config-radsrv-group)#policy vlan 10
5. Use the **policy wlan** command to allow only authorized users to access this group's WLAN.
   RFController(config-radsrv-group)#policy wlan 1 2 5
6. Use **(config-radsrv)#rad-user** to create a user called testuser and add it to the group.
   ```
   RFController(config-radsrv)#rad-user testuser password testpassword group
   sales
   Mar 07 17:41:55 2008: RADCONF: Adding user "testuser" into local database
   Mar 07 17:41:55 2008: RADCONF: User "testuser" is added to group "sales"
   ```
7. Use **(config-radsrv)#nas** to add a NAS entry for the group.
   ```
   RFController(config-radsrv)#nas ?
   A.B.C.D/M  Radius client IP address

   RFController(config-radsrv)#nas 10.10.10.0/24 ?
   key  Radius client shared secret

   RFController(config-radsrv)#nas 10.10.10.0/24 key ?
   0     Password is specified UNENCRYPTED
   2     Password is encrypted with password-encryption secret
   LINE  The secret(client shared secret), upto 32 characters

   RFController(config-radsrv)#nas 10.10.10.0/24 key 0 very-secret!!
   ```
8. Use **(config-radsrv)#proxy** to add a realm name for the group.
   ```
   RFController(config-radsrv)#proxy realm mydomain.com server 10.10.1.10
   port 1812 secret 0 testing
   ```

9. Save the changes and restart the RADIUS server.

```
RFController(config-radsrv)#service radius restart
Mar 07 17:48:04 2010: %PM-5-PROCSTOP: Process "radiusd" has been stopped
Mar 07 17:48:05 2010: RADCONF: radius config files generated successfully
RFController(config-radsrv)#Mar 07 17:48:05 2010: %DAEMON-6-INFO:
radiusd[8830]: Ready to process requests.
```

help

Radius configuration commands

Displays the system's interactive help in HTML format

Supported in the following platforms:

- Mobility RFS4000 Controller
- Mobility RFS6000 Controller
- Mobility RFS7000 Controller

Syntax

```
help
```

Parameters

None

Example

```
RFController(config-radsrv)#help?
  help  Description of the interactive help system

RFController(config-radsrv)#help
CLI provides advanced help feature.  When you need help,
anytime at the command line please press '?'.

If nothing matches, the help list will be empty and you must backup
until entering a '?' shows the available options.
Two styles of help are provided:
1. Full help is available when you are ready to enter a
   command argument (e.g. 'show ?') and describes each possible
   argument.
2. Partial help is provided when an abbreviated argument is entered
   and you want to know what arguments match the input
   (e.g. 'show ve?'.)

RFController(config-radsrv)#
```

ldap-server

Radius configuration commands

Sets the LDAP server configuration

It uses the existing external database (active directory with the onboard RADIUS server) instead of the local database on the controller.

Supported in the following platforms:

- Mobility RFS4000 Controller
- Mobility RFS6000 Controller
- Mobility RFS7000 Controller

Syntax

```
ldap-server [primary|secondary] host <IP>

ldap-server primary host <IP> port <1-65535>
login <user-name> bind-dn <distinguished-name> base-dn
<distinguished-name> passwd {<password>|<password>
|<password>} passwd-attr <password-attribute>
group-attr <group-attribute> group-filter
<group-filter> group-membership <group> net-timeout <1-10>

ldap-server secondary host <IP> port <1-65535> login <user-name> bind-dn
<distinguished-name> base-dn <distinguished-name> passwd
{<password>|<password>|
<password>} passwd-attr <password-attribute>
group-attr <group-attribute> group-filter <group-filter> group-membership
<group> net-timeout <1-10>
```

Parameters

ldap-server primary host <IP> port <1-65535> login <user-name> bind-dn <distinguished-name> base-dn <distinguished-name> passwd {<password>|<password>|<password>} passwd-attr <password-attribute> group-attr <group-attribute> group-filter <group-filter> group-membership <group> net-timeout <1-10>	Sets the primary LDAP server's configuration
	• host < IP> – Sets the LDAP server's IP configuration
	  • <IP> – Defines the LDAP server IP address
	  • port <number> – Enter the TCP/IP port number for the LDAP server acting as the data source
	  • login <user-name> – Use the following as the login: `(sAMAccountName=%{Stripped-User-Name:-%{User-Name}})`
	  • bind-dn <distinguished-name> – Specifies the distinguished name to bind with the LDAP server
	  • base-dn <distinguished-name> – Specifies a distinguished name that establishes the base object for the search. The base object is the point in the LDAP tree at which to start searching.
	  • passwd {<password>|<password>|<password>} – Sets a valid password for the LDAP server
	  • passwd-attr <password-attribute> – Enter the password attribute used by the LDAP server for authentication
	  • group-attr <group-attribute> – Specifies the group attribute used by the LDAP server
	  • group-filter <group-filter> – Specifies the group filters used by the LDAP server
	  • group-membership <group> – Specifies the Group Member Attribute sent to the LDAP server when authenticating users
	  • net-timeout<1-10> – Enter a timeout the system uses to terminate the connection to the RADIUS Server if no activity is detected

ldap-server secondary host <IP> port <1-65535> login <user-name> bind-dn <distinguished-name> base-dn <distinguished-name> passwd {<password>|<password>|<password>} passwd-attr <password-attribute> group-attr <group-attribute> group-filter <group-filter> group-membership <group> net-timeout <1-10>	Defines the secondary LDAP server's configuration.

Usage Guidelines

Use the login filter and group filter values (described in the example below) for all LDAP configuration scenarios

Use the `passwd` parameter to enter the password for the active directory user mentioned in bind -dn. This is used for the initial login to the active directory.

The `passwd-attr` and `group-membership` is retained as described in the following example:

Example

```
RFController(config)#ldap-server primary host xxx.xxx.x.xx port 389 login
(sAMAccountName=%{Stripped-User-Name:-%{User-Name}}) bin
d-dn cn=admin,ou=wid,dc=brocadeTech,dc=local base-dn
ou=wid,dc=brocadeTech,dc=local passwd brocade@123 passwd-attr UserPassword
group-attr cn group-filter
(|(&(objectClass=group)(member=%{Ldap-UserDn}))(&(objectClass=GroupOfUniqueNa
mes)(uniquemember=%{L
dap-UserDn}))) group-membership radiusGroupName net-timeout 1
RFController(config)#
```

nas

Radius configuration commands

Sets the configuration of the RADIUS client

Supported in the following platforms:

- Mobility RFS4000 Controller
- Mobility RFS6000 Controller
- Mobility RFS7000 Controller

Syntax

```
nas <IP/Mask> key [0<key>|2<key>|<key>]
```

Parameters

<IP/Mask>	Sets the RADIUS client's IP address
[0<key>|2<key>|<key>]	Sets the RADIUS client's shared key • 0 – Defines the Password as UNENCRYPTED • 2 – Password is encrypted with password-encryption secret • LINE – Defines the secret (client shared secret) up to 32 characters

Example

```
RFController(config-radsrv)#nas ?
A.B.C.D/M  Radius client IP address

RFController(config-radsrv)#nas 10.10.10.0/24 ?
key  Radius client shared secret

RFController(config-radsrv)#nas 10.10.10.0/24 key ?
0     Password is specified UNENCRYPTED
2     Password is encrypted with password-encryption secret
LINE  The secret(client shared secret), upto 32 characters

RFController(config-radsrv)#nas 10.10.10.0/24 key 0 very-secret!!
```

no

Radius configuration commands

Negates a command or sets its defaults

Supported in the following platforms:

- Mobility RFS4000 Controller
- Mobility RFS6000 Controller
- Mobility RFS7000 Controller

Syntax

```
no [authentication|ca|crl-check|group|ldap-server|nas|proxy|
rad-user|server]
```

Parameters

None

Example

```
RFController(config-radsrv)#no authentication data-source
RFController(config-radsrv)#

RFController(config-radsrv)#no ca trust-point
RFController(config-radsrv)#
```

proxy

Radius configuration commands

Configures a proxy RADIUS server based on the realm/suffix

Supported in the following platforms:

- Mobility RFS4000 Controller
- Mobility RFS6000 Controller
- Mobility RFS7000 Controller

Syntax

```
proxy [realm|retry-count|retry-delay]
proxy realm <realm-name> server <IP> port <1024-65535>
secret{<secret>|<secret>|<secret>}
```

Parameters

realm <realm-name> server <IP> port <1024-65535> secret {<secret>|<secret>|<secret>}	The realm name is a string of up to 50 characters
	• server <IP> – Sets the proxy server IP address
	• port <1024-65535> – Sets the proxy server port number
	• secret {<secret>|<secret>|<secret>} – Sets the proxy server secret string
	  • <secret> – Password is specified UNENCRYPTED
	  • <secret> – Password is encrypted with a password encryption secret
	  • <secret> – Sets the proxy server shared secret up to 32 characters

retry-count <3-6>	Defined the proxy server retry count value
retry-delay<5-10>	Defines the proxy server retry delay time (in seconds)

Usage Guidelines

Only five RADIUS proxy servers can be configured. The proxy server attempts six retries before it times out. The retry count defines the number of times the controller transmits each RADIUS request before giving up. The timeout value defines the duration for which the controller waits for a reply to a RADIUS request before retransmitting the request.

Example

```
RFController(config-radsrv)#proxy realm Test server 10.10.10.1 port 2220
secret "Very Very Secret !!!"
RFController(config-radsrv)#

RFController(config-radsrv)#proxy retry-count 5
RFController(config-radsrv)#

RFController(config-radsrv)#proxy retry-delay 8
RFController(config-radsrv)#
```

rad-user

Radius configuration commands

Sets RADIUS user parameters

Supported in the following platforms:

- Mobility RFS4000 Controller
- Mobility RFS6000 Controller
- Mobility RFS7000 Controller

Syntax

```
rad-user <user-name>
rad-user <user-name> [access|password|privilege]
rad-user <user-name> access [console|ssh|telnet|web]
rad-user <user-name> password [0<password>|2<password>
|<password>] group guest expiry-time <HH:MM> expiry-date <MM:DD:YYYY>
start-time <HH:MM> start-date <MM:DD:YYYY>] access-duration <duration time>]
rad-user <user-name> privilege [helpdesk|monitor|
nwadmin|superuser|sysadmin|webadmin]
```

Parameters

<user-name> [access|console|ssh |telnet|web>]	Enter a user name up to 64 characters in length
	• access [console|ssh|telnet|web>] – Set management user access mode
	  • console – Only allowed from console
	  • ssh – Only allowed from ssh
	  • telnet – Only allowed from telnet
	  • web – Only allowed from applet

password [0<password>|2<password >|<password>] group guest expiry-time <HH:MM> expiry-date <MM:DD:YYYY> start-time <HH:MM> start-date <MM:DD:YYYY>] access-duration <30-35791390>	Sets the RADIUS user password
	• 0 <password> – Defines the password as UNENCRYPTED
	• 2 <password> – The password is encrypted with a password encryption secret
	• <password> – Sets a password up to 21 characters in length
	  • group – Radius server group configuration
	  • <group-name> – Existing group name in local database
	  • guest – Enable guest user access
	  • expiry-time <HH:MM> – Time of expiry
	  • expiry-date <MM:DD:YYYY> – Date of expiry
	  • start-time <HH:MM> – User account activation time
	  • start-date <MM:DD:YYYY> – User access start date
	  • access-duration - Defines allowed time in minutes
	  • <30-35791390> - Defines the access duration time

privilege [helpdesk|monitor| nwadmin|superuser| sysadmin|webadmin]	Set management user access privilege • helpdesk [monitor|nwadmin|superuser|sysadmin|webadmin]– helpdesk (troubleshooting) access • monitor [helpdesk|nwadmin|superuser|sysadmin|webadmin]– Monitor (read-only) access • nwadmin [helpdesk|monitor|superuser|sysadmin|webadmin]– Network (wired&wireless) admin access superuser[helpdesk|monitor|nwadmin|sysadmin|webadmi n– Superuser (root) access • sysadmin [helpdesk|monitor|nwadmin|superuser|webadmin] – System <general system configuration>admin access • webadmin [helpdesk|monitor|nwadmin|superuser|sysadmin]– Web auth (hotspot) user admin access

Usage Guidelines

Use `group, guest, expiry-time expiry-date, start-time` and `start-date` parameters to create a RADIUS guest user.

The RADIUS user group specified while creating a guest user must be a *guest-group*.

Example

```
RFController(config-radsrv)#rad-user TestRadUser password "I SPY U"
RFController(config-radsrv)#

RFController(config-radsrv)#rad-user guest1 password 0 password1 group
guest-group
guest expiry-time 12:12 expiry-date 05:12:2010 start-time 12:12 start-date
05:11:2010
RFController(config-radsrv)#
```

server

Radius configuration commands

Configures server certificate parameters used by a RADIUS server

The server certificate is a part of a trustpoint created using *crypto on page 233*.

Supported in the following platforms:

- Mobility RFS4000 Controller
- Mobility RFS6000 Controller
- Mobility RFS7000 Controller

Syntax

```
server trust-point <trust-point name>
```

Parameters

server trust-point <trust-point name>	Configures server certificate parameters • trust-point <trust-point name> – Sets the trustpoint configuration • <trust-point name> – Existing trustpoint name

Usage Guidelines

Create a trustpoint using **`(crypto-pki-trustpoint)`**. The server certificate must be created under the trustpoint using crypto-pki commands. Refer to *crypto on page 233* for more information.

Example

```
RFController(config-radsrv)#server trust-point TestTP
RFController(config-radsrv)#
```

service

Radius configuration commands

Invokes the service commands to troubleshoot or debug the `(config-radsrv)` instance configuration

This command is also used to enable the RADIUS server.

Supported in the following platforms:

- Mobility RFS4000 Controller
- Mobility RFS6000 Controller
- Mobility RFS7000 Controller

Syntax

```
service show cli
```

Parameters

None

Example

```
RFController(config-radsrv)#service show cli
Radius Configuration mode:
+-authentication
  +-data-source
    +-ldap [authentication data-source (local|ldap)]
    +-local [authentication data-source (local|ldap)]
  +-eap-auth-type
    +-all [authentication eap-auth-type
(ttls-md5|ttls-pap|ttls-mschapv2|peap-gt
c|peap-mschapv2|tls|all)]
    +-peap-gtc [authentication eap-auth-type
(ttls-md5|ttls-pap|ttls-mschapv2|pe
ap-gtc|peap-mschapv2|tls|all)]
    +-peap-mschapv2 [authentication eap-auth-type
(ttls-md5|ttls-pap|ttls-mschap
v2|peap-gtc|peap-mschapv2|tls|all)]
    +-tls [authentication eap-auth-type
(ttls-md5|ttls-pap|ttls-mschapv2|peap-gt
c|peap-mschapv2|tls|all)]
    +-ttls-md5 [authentication eap-auth-type
(ttls-md5|ttls-pap|ttls-mschapv2|pe
ap-gtc|peap-mschapv2|tls|all)]
    +-ttls-mschapv2 [authentication eap-auth-type (ttls-md5|ttls-
```

show

Radius configuration commands

Displays current system information running on the controller

Supported in the following platforms:

- Mobility RFS4000 Controller
- Mobility RFS6000 Controller
- Mobility RFS7000 Controller

NOTE
The following commands display only for the Mobility RFS6000 Controller and the Mobility RFS4000 Controller
- power
The following commands display only for the Mobility RFS7000 Controller and the Mobility RFS4000 Controller:
- port-channel
- static-channel-group

Syntax

```
show <paramater>
```

Parameters

?	Displays the parameters for which information can be viewed using the show command

Example

```
RFController(config-radsrv)#show ?
  access-list           Internet Protocol (IP)
  aclstats              Show ACL Statistics information
  alarm-log             Display all alarms currently in the system
  autoinstall           autoinstall configuration
  banner                Display Message of the Day Login banner
  boot                  Display boot configuration.
  clock                 Display system clock
  commands              Show command lists
  crypto                encryption module
  debugging             Debugging information outputs
  dhcp                  DHCP Server Configuration
  environment           show environmental information
  file                  Display filesystem information
  firewall              Wireless firewall
  ftp                   Display FTP Server configuration
  history               Display the session command history
  interfaces            Interface status
  ip                    Internet Protocol (IP)
  ldap                  LDAP server
  licenses              Show any installed licenses
  logging               Show logging configuration and buffer
  mac                   Internet Protocol (IP)
  mac-address-table     Display MAC address table
  mac-name              Displays the configured mac names
  management            Display L3 Managment Interface name
```

```
  mobility              Display Mobility parameters
  ntp                   Network time protocol
  password-encryption   password encryption
  port                  Physical/Aggregate port interface
  port-channel          Portchannel commands
  privilege             Show current privilege level
  protocol-list         List of protocols
  radius                RADIUS configuration commands
  redundancy            Display redundancy group parameters
  rtls                  Real Time Locating System commands
  role                  Configure role parameters
  running-config        Current Operating configuration
  securitymgr           Securitymgr parameters
  service-list          List of services
  sessions              Display current active open connections
  smtp-notification     Display SNMP engine parameters
  snmp                  Display SNMP engine parameters
  snmp-server           Display SNMP engine parameters
  spanning-tree         Display spanning tree information
  startup-config        Contents of startup configuration
  static-channel-group  static channel group membership
  terminal              Display terminal configuration parameters
  timezone              Display timezone
  traffic-shape         Display traffic shaping
  upgrade-status        Display last image upgrade status
  users                 Display information about currently logged
                        in users
  version               Display software & hardware version
  virtual-ip            IP redundancy list
  wireless              Wireless configuration commands
  wlan-acl              wlan based acl
RFController(config-radsrv)#show
```

ldap-group-verification

Radius configuration commands

Displays ldap group verification settings

Supported in the following platforms:

- Mobility RFS4000 Controller
- Mobility RFS6000 Controller
- Mobility RFS7000 Controller

Syntax

```
ldap-group-verification [disable|enable]
```

Parameters

ldap-group-verification [disable|enable]	Displays ldap group verification settings • disable – Disables group verification • enable – Enables group verification

Example

```
RFController(config-radsrv)#ldap-group-verification disable
RFController(config-radsrv)#
```

Chapter

20

Wireless Instance

In this chapter

Use the `(config-wireless)` instance to configure local RADIUS server parameters associated with the controller.

To navigate to this instance, use the command from the Global Config mode.

```
RFController(config)#wireless
RFController(config-wireless)#
```

Wireless configuration commands

This table summarizes **`(config-wireless)`** commands:

TABLE 22 Wireless Configuration Commands

Command	Description	Ref.
aap	Sets *Adaptive AP* (AAP) related commands	*page 592*
admission-control	Enable admission control across all radios	*page 594*
adopt-unconf-radio	Adopts a radio even if its not yet configured. The default templates can be used for configuration.	*page 595*
adoption-pref-id	Used as a preference identifier for this controller. All radios configured with this preference identifier are more likely to be adopted by this controller.	*page 596*
ap	Displays access point related commands	*page 597*
ap-containment	Defines the Rogue AP containment configuration	*page 602*
ap-detection	Defines the AP detection configuration	*page 603*
ap-image	Defines the path to upload the new image over an AP	*page 604*
ap-ip	Modifies static IP information for access points	*page 605*
ap-standby-attempts-threshold	Sets the number of attempts after which the stand-by controller starts adopting APs	*page 607*
ap-timeout	Changes the default inactivity timeout for access points	*page 608*
ap-udp-port	Configures the UDP port for AP L3 adoption. Enable this option in the DHCP Server supporting this access-point.	*page 609*
auto-select-channels	Configures the channels that will be used when ACS or DFS is performed.	*page 610*

TABLE 22 Wireless Configuration Commands

Command	Description	Ref.
broadcast-tx-speed	Sets the rate at which broadcast and multicast traffic is transmitted	*page 611*
client	Defines the wireless client configuration	*page 612*
clrscr	Clears the display screen	*page 615*
cluster-master-support	Changes settings for cluster master support. This is required for cluster-level functions	*page 616*
convert-ap	Changes an AP's mode of operation	*page 617*
country-code	Configures the country of operation. All existing radio configurations are erased.	*page 619*
debug	Debugging functions.	*page 620*
dhcp-one-portal-forward	Enables forwarding of DHCP responses to one portal.	*page 623*
dhcp-sniff-state	Records wireless client DHCP state information	*page 624*
dot11-shared-key-auth	Enables support for 802.11 shared key authentication	*page 625*
end	Ends the current mode and moves to the EXEC mode	*page 626*
exit	Ends the current mode and moves to the previous mode	*page 627*
fix-broadcast-dhcp-rsp	Converts broadcast DHCP server responses to unicast responses	*page 628*
help	Displays the interactive help system	*page 629*
hotspot	Configures Hotspot configuration information.	*page 630*
load-balance	Sets the user load balance mode	*page 631*
mac-auth-local	Defines the local MAC authentication list	*page 632*
manual-wlan-mapping	Allows the manual mapping/un-mapping of WLANs to configured radios	*page 634*
wireless-client	Configures wireless client parameters	*page 635*
mobility	Configures mobility parameters	*page 636*
multicast-packet-limit	Sets a multicast packet limit (per second) for a VLAN	*page 637*
multicast-throttle-watermark	Configures watermarks for handling bursts of broadcast/multicast frames	*page 638*
nas-id	Configures the NAS ID to be sent to the RADIUS server.	*page 639*
nas-port-id	Configures the NAS port to be sent to the RADIUS server.	*page 640*
no	Negates a command or sets its defaults	*page 641*
proxy-arp	Responds to ARP requests from the RON to a WLAN on behalf of clients	*page 642*

TABLE 22 Wireless Configuration Commands

Command	Description	Ref.
qos-mapping	Defines the QoS mapping between wired and wireless domains	*page 643*
radio	Defines the radio's configuration	*page 644*
rate-limit	Sets the default rate limit (per user)	*page 655*
secure-wispe-default-secret	Configure default shared secret for secure wispe	*page 656*
self-heal	Sets the self healing configuration	*page 657*
sensor	Defines the *Wireless Intrusion Protection System* (WIPS) configuration	*page 659*
service	Invokes service commands to troubleshoot or debugs the `(config-wireless)` instance configuration	*page 661*
show	Displays running system information	*page 671*
smart-rf	Config Smart-RF Management Parameters	*page 679*
smart-scan-channels	Specify a list channels to brocade clients to perform smart-scan	*page 680*
wlan	Sets WLAN related parameters	*page 681*
wlan-bw-allocation	Allocates radio bandwidth (per WLAN)	*page 698*

aap

Wireless configuration commands

Defines the AAP configuration

Supported in the following platforms:

- Mobility RFS4000 Controller
- Mobility RFS6000 Controller
- Mobility RFS7000 Controller

NOTE
The number of AAPs supported differ from controller to controller.
- Mobility RFS7000 Controller – Supports up to 1024 AAPs
- Mobility RFS6000 Controller – Supports up to 256 AAPs
- Mobility RFS4000 Controller – Supports up to 6 AAPs

Syntax

```
aap [aap-version|auto-upgrade|config-apply|fwupdate|include-config]
aap aap-version [br7131] <version-number>
aap auto-upgrade enable
aap config-aaply [def-delay|mesh-delay] <3-10000>
aap fwupdate [<1-256>|<LIST>|filename|ipaddress|location|mode|
password|staggercount|unadopted|username
```

Parameters

aap-version [br7131] <version-number>	Enables version number • br7131 • <version-number> – Configures minimum ap version required for adoption. A firm version string in the format X.X.X.X-XXXR
auto-upgrade enable	Enables automatic firmware upgrade of Adaptive AP on the controller

config-apply [def-delay|mesh-delay] <30-10000>	Applies AAP configuration settings
	• def-delay – Sets the default time to delay before applying AAP configuration
	  • <30 -10000> – Set the delay time (in seconds)
	• mesh-delay – Defines the interval to delay before applying AAP configuration to Mesh APs
	  • <3--10000> – Set the delay time (in seconds)

fwupdate [<1-256>| <LISt> |ip-address|location|mode password|stagger-count| unadopted|username]	Manually upgrades the specified Advanced AP. The options are: • <1-256> – Updates the AAP based on its index number • <LIST> – Updates the AAP based on its MAC Address. An AAP can be updated based on either a single MAC address or a list of MAC addresses or a range of MAC addresses. Use the `show wireless ap` command to view the AP index • ip-address – Sets the remote SFTP server IP address . • location – Specifies the path name of the firmware image in the remote SFTP server • mode – Firmware upgrade mode ftp/sftp. Default is ftp. • password – SFTP server password • stagger-count <1-10> – Configure simultaneous upgrade count • <1-10> – Number of simultaneous upgrades to perform. • unadopted – Updates the unadopted AAPs • username – Username to login to the SFTP server.

Usage Guidelines

Use **`{no} aap auto-upgrade enable`** to disable the auto-upgrade facility on the controller

Example

```
RFController(config-wireless)#aap config-apply mesh-delay 300
RFController(config-wireless)#

RFController(config-wireless)#aap fwupdate mode test
aap fwupdate mode test
RFController(config-wireless)#

RFController(config-wireless)#aap fwupdate stagger-count 1
RFController(config-wireless)#
```

admission-control

Wireless configuration commands

Enable admission control for voice traffic across all radios

Supported in the following platforms:

- Mobility RFS4000 Controller
- Mobility RFS6000 Controller
- Mobility RFS7000 Controller

Syntax

```
admission-control voice enable
```

Parameters

voice enable	Enables admission control for voice on all radios.

Usage Guidelines

Use **{no} admission-control voice enable** to disable Admission Control for voice or video on all radios.

Example

```
RFController(config-wireless)#admission-control voice enable
RFController(config-wireless)#
```

adopt-unconf-radio

Wireless configuration commands

Adopts a radio (even if not yet configured). Default templates are used for configuring the adopted radio

Supported in the following platforms:

- Mobility RFS4000 Controller
- Mobility RFS6000 Controller
- Mobility RFS7000 Controller

Syntax

```
adopt-unconf-radio enable
```

Parameters

None

Usage Guidelines

Use the **{no} adopt-unconf-radio** command to switch off adopting unconfigured radios.

Example

```
RFController(config-wireless)#adopt-unconf-radio enable
RFController(config-wireless)#
```

adoption-pref-id

Wireless configuration commands

Preference identifier for the controller

All radios configured with this preference identifier are more likely to be adopted by this controller.

Supported in the following platforms:

- Mobility RFS4000 Controller
- Mobility RFS6000 Controller
- Mobility RFS7000 Controller

Syntax

```
adoption-pref-id <pref-id>
```

Parameters

<pref-id>	Set a preference ID with a numeric value in the range of 1-65535

Example

```
RFController(config-wireless)#adoption-pref-id 500
RFController(config-wireless)#
```

ap

Wireless configuration commands

Defines the name, location and other parameters of access points

Supported in the following platforms:

- Mobility RFS4000 Controller
- Mobility RFS6000 Controller
- Mobility RFS7000 Controller

Syntax

```
ap [<1-256>|<LIST>|<MAC-ADDRESS>] [ABG Scan|aap-log-storage|aap-admin-passwd|
||adoption-policy|
|aap-ipfilter-list|aap-lan1-ipf-rules
|aap-lan1-trunking|aap-syslog-srvr|country-code|lan-acl|location|name|radio-c
onfig|secure-mode||secure-mode-staging]
ap <1-256> aap-admin-passwd <LINE>

ap <1-256> aap-log-storage enable
ap <1-256> aap-syslog-srvr enable level <0-7> ipaddr
ap <1-256> adoption-policy [allow|deny]
ap <1-256> country-code <country-code>
ap <1-256> leds (enable)

ap <1-256> location <location>
ap <1-256> name <name>
ap <1-256> secure-mode [enable|secret [0 <secret>|2 <secret>|<secret>]
ap <1-256> secure-mode-staging enable
ap <1-256> aap-ipfilter-list <AAP-IPFiltername>
ap <1-256> aap-lan1-ipf-rules [in|out] {<1-20>|<AAP_IP_RULE>}
ap <1-256> aap-lan1-trunking [disable|enable mgmt-vlan-id
       <1-4094> native-vlan-id <1-4094> native-tagging [tagged|untagged]]

ap <LIST> adoption-policy [allow|deny]
ap <LIST> aap-log-storage enable
ap <LIST> aap-syslog-srvr enable level <0-7> ipaddr
ap <LIST> country-code <country-code>

ap <LIST> leds (enable)
ap <LIST> location <location>
ap <LIST> name <name>
ap <LIST> secure-mode [enable|secret [0 <secret>|2 <secret>|<secret>

ap <LIST> secure-mode-staging enable
ap <MAC-ADDRESS> aap-admin-passwd

ap <MAC-ADDRESS> adoption-policy [allow|deny]
ap <MAC-ADDRESS> aap-log-storage enable
ap <MAC-ADDRESS> aap-syslog-srvr (enable)(level)<0-7> <ipaddr>
ap <MAC-ADDRESS> country-code <country-code>

ap <MAC-ADDRESS> location <location>
ap <LIST> leds (enable)
ap <MAC-ADDRESS> name <name>
ap <MAC-ADDRESS> secure-mode [enable|secret [0 <secret>|2 <secret>|<secret>]
ap <MAC-ADDRESS> secure-mode-staging enable
```

```
ap <MAC-ADDRESS> aap-ipfilter-list <AAP-IPFiltername>
ap <MAC-ADDRESS> aap-lan1-ipf-rules [in|out] {<1-20>|<AAP_IP_RULE>}
ap <MAC-ADDRESS> aap-lan1-trunking [disable|enable mgmt-vlan-id
       <1-4094> native-vlan-id <1-4094> native-tagging [tagged|untagged]]

ap <MAC-ADDRESS> radio-config [2-4-wlan-5-0-wlan|2-4-wlan-5-0-wlan-sensor|
    2-4-wlan-only|2-4-wlan-sensor|5-0-wlan-only|
    5-0-wlan-sensor|all-radios-off|sensor-only]
```

Parameters

<1-256>
[ABG Scan|adoption-policy|aap-admin-passwd||aap-log-storage|aap-syslog-srvr|country-code|leds|location|name|secure-code|secure-mode-stagging|aap-ipfilter-list |aap-lan1-ipf-rules|aap-lan1-trunking]
	Sets a single AP index. Use the `show wireless ap` command to view the AP's index value.
	• ABG Scan enable – Configures the ABG scan mode on the AP
	• enable – Allows detector radio to perform ABG scan
	• adoption-policy [allow|deny]– Specifies adoption policy
	  • allow – Allow adoption
	  • deny – Deny adoption
	• aap-log-storage (enable) – Configure storage of AAP log messages file
	  • enable – Enables storage
	• aap-syslog-srvr (enable) (level <0-7> <ipaddr>)– Configures aap syslog output.
	  • enable – Enables syslogging
	  • level <0-7> – Specify syslog level
	  • ipaddr – Specify server IP address
	• country-code <country-code> – Defines the country of operation for the ap. Regulatory configurations such as channels will be configured automatically.
	• leds (enable) – Configures ap LEDs
	  • enable – Enables LEDs
	• location <location> – Defines the location description of the AP
	• <location> – A string of upto 40 charactersname <name> – Sets the name of this AP
	  • <name> – A string of upto 40 characters
	• secure-mode [enable|secret] – WISPe secure mode. Configures a shared secret to a set of APs (specified by LIST). The AP's MAC, shared secret will be saved in the running configuration file. If this command is not executed for an AP, default pre-shared secret will be assigned.
	  • enable – Configure secure-mode to a set of APs (specified by LIST). The AP's MAC and mode will be saved in the running configuration.
	  If secure-mode is enabled, the WISP-e for this AP is secured
	  • secret [0 <secret>|2 <secret>|<secret>] – Secret is a string of up to 64 characters
	  • 0 – Password is specified UNENCRYPTED
	  • 2 – Password is specified encrypted with password-encryption secret
	  • <secret> – If the secret <secret> is not specified then default secret will be used
	• secure-mode-staging enable – WISPe secure mode staging
	  • enable – Configure secure-mode staging to a set of APs (specified by LIST). The AP's MAC, and staging mode will be saved in the running configuration.
	  In this mode, controller will send configured shared secret in the clear in the Join response to the AP.
	  • Use the `{no} secure-mode-staging enable` command to negate.
	• aap-admin-passwd – Configure aap admin password
	• aap-ipfilter-list – Configures aap IP filter listaap-lan1-ipf-rules – Configures aap Lan 1 IP filter rules.

	• aap-lan1-trunking [disable|enable] – Configures trunking on LAN1 of AAP
	  • disable – Disables trunking on AAP LAN 1 inerface
	  • enable mgt-valn-id – Enables trunking on AAP LAN 1 inerface
	  • mgmt-vlan-id <1-4094> native -vlan-id – Configures management VLAN ID on AAP between 1 and 4094
	  • native-vlan-id <1-4094> native-tagging – Configures native VLAN ID on AAP between 1 and 4094
	  • native-tagging [tagged|untagged] – Configures native VLAN tagging on AAP between 1 and 4094
	  • tagged – Enables native VLAN tagging on AAP LAN 1 inerface
	  • untagged – Disables native VLAN tagging on AAP LAN 1 inerface

<LIST> [ABG-Scan|aap-admin-passwd|aap-log-storage|aap-syslog-srvr|adoption-policy| country-code| location|leds| name|secure-code| secure-mode-stagging|aap-ipfilter-list | aap-lan1-ipf-rules|aap-lan1-trunking]	A list (eg: 1,3,7) or range (eg: 3-7) of AP indices from the `show wireless ap` command
<MAC-address> [ABD-Scan|aap-admin-passwd|aap-log-storage|aap-syslog-srvr|adoption-policy| country-code |location|ledsl| name|radio-config| secure-code| secure-mode-stagging|aap-ipfilter-list | aap-lan1-ipf-rules|aap-lan1-trunking]	Lists an AP's MAC address.

Usage Guidelines

Use `{no} ap <LIST> secure-mode secret` to reset a shared secret for a set of APs (specified by LIST) to the default shared secret. It is saved in the running configuration file.

Use `{no} ap <list> secure-mode enable` to disable secure-mode to a set of APs (specified by LIST). The AP's MAC, and mode will be saved in the running configuration.

Use `{no} ap <list> secure-mode-staging enable` to disable secure-mode staging to a set of APs (specified by LIST). The AP's MAC, and staging mode will be saved in the running configuration. In this mode, controller will not send at all configured shared secret in the Join response to the AP and AP will not get adopted by the controller.

Example

```
RFController(config-wireless)#ap 00-15-70-14-FE-C4 location 5th Floor
SalesUnit
RFController(config-wireless)#ap 1 location SJ NewPark
RFController(config-wireless)#
```

ap-containment

Wireless configuration commands

Sets the rogue AP containment parameters

Supported in the following platforms:

- Mobility RFS4000 Controller
- Mobility RFS6000 Controller
- Mobility RFS7000 Controller

Syntax

```
ap-containment [add <MAC>|enable|interval <interval>)
```

Parameters

add <MAC>	Adds an AP's MAC Address <MAC> into the rogue AP containment list.
enable	Enables the Rogue AP Containment feature.
interval <interval>	Sets the time <interval>, a value in the rage of 20-5000, between two Rogue AP containment processes. Time duration is in milliseconds.

Example

```
RFController(config-wireless)#ap-containment enable
RFController(config-wireless)#ap-containment interval 300
RFController(config-wireless)#ap-containment add 00-15-70-37-fa-be
RFController(config-wireless)#
```

NOTE
The effective ap -containment interval for APs is 200ms which is channel dwell time. This remains same even if it configured to a lower value. For single-scan-APs, the smaller values of containment will be effective.

ap-detection

Wireless configuration commands

Configures access point detection parameters

Supported in the following platforms:

- Mobility RFS4000 Controller
- Mobility RFS6000 Controller
- Mobility RFS7000 Controller

Syntax

```
ap-detection [add|detect-wired-rouge|enable| mu-assisted-scan|timeout]
ap-detection  add <list-index>[authorized|ignored] [<MAC>|any] <LINE>|any]
ap-detection detect-wired-rouge enable
ap-detection enable
ap-detection mu-assisted-scan [enable|refresh <refresh-period>]
ap-detection timeout [authorized|unauthorized|ignored] <timeout>
```

Parameters

approved add <list-index> [<MAC>|any]	Sets the approved access point list • add <list-index> – Adds an entry to the approved access point list at the index <list-index>. • <MAC> – The a MAC address <MAC> in AA-BB-CC-DD-EE-FF format. • any– Assigns any MAC address.
enable	Allows access points to look for APs
client-assisted-scan [enable| refresh <refresh-period>]	Sets wireless client assisted scanning configuration • enable – Enables wireless client assisted scanning • refresh <refresh-period>> – Defines the period <refresh-period> (300 – 86400) (in seconds) used by all scan-capable wireless clients are polled to scan for neighboring access points.
ap-detection timeout [approved|unapproved] <timeout>	Sets the amount of time (in seconds) an AP remains in the list after it is no longer seen • approved <timeout> – The timeout <timeout> in seconds for approved APs. • unapproved <timeout> – The timeout <timeout> in seconds for unapproved APs

Example

```
RFController(config-wireless)#ap-detection enable
RFController(config-wireless)#

RFController(config-wireless)#ap-detection authorized add 150 any any
RFController(config-wireless)#

RFController(config-wireless)#ap-detection client-assisted-scan enable
RFController(config-wireless)#

RFController(config-wireless)#ap-detection client-assisted-scan refresh 520
RFController(config-wireless)#
```

ap-image

Wireless configuration commands

Defines the path to upload the new image over an AP

Supported in the following platforms:

- Mobility RFS4000 Controller
- Mobility RFS6000 Controller
- Mobility RFS7000 Controller

Syntax

```
ap-image [br300-ids-sensor|br300-wisp|br300-wispe|br650-wispe|
          br7131] <file-path>
```

Parameters

[br300-ids-sensor| br300-wisp| br300-wispe| br300-wispe| |br7131] <file-path>	The interface to upload new AP image. The following APs are supported: • br300-ids-sensor – IDS Sensor firmware for BR300 • br300-wisp – WISP image for BR300 • br300-wispe – WISPe image for BR300 • br650-wispe – WISPe image for BR650 • br7131 – Adaptive AP image for BR7131 • <file-path> – Path of the new AP-Image

Example

```
RFController (config-wireless)#ap-image br7131 flash:/aap_10B.bin
RFController (config-wireless)#
```

ap-ip

Wireless configuration commands

Modifies the static IP address for an access point

Supported in the following platforms:

- Mobility RFS4000 Controller
- Mobility RFS6000 Controller
- Mobility RFS7000 Controller

Syntax

```
ap-ip [<AP-list/MAC>|default-ap]

ap-ip <AP-list/MAC> [static-ip|controller-ip]
ap-ip <AP-list/MAC> static-ip <IP/Mask> <gateway-IP>
ap-ip <AP-list/MAC> controller-ip [add <IP>|
delete [<IP>|<IP-index>]|<IP>|set-default]
ap-ip default-ap controller-ip [add <IP address>|delete [<IP|<IP-index>]|
<IP address>)|set-default]
```

Parameters

ap-ip <AP-list/MAC> [static-ip|controller-ip]	Use show wireless ap to view an AP's index or MAC address. Select the AP's index / MAC Address to modify its static IP address.
	• static-ip <IP/Mask> <gateway-IP> – Sets the static IP address, netmask and gateway address of the AP
	  • <IP/Mask> – Defines the static IP address and mask
	  • <gateway-IP>– Sets the gateway IP address
	• controller-ip [add <IP>| delete [<IP>|<IP-index>]|<IP>|set-default] – Defines the static controller IP address
	  • add <IP> – Adds a static controller IP address <IP>
	  • delete [<IP-index>|<IP>] – Deletes a static controller IP address
	  • <IP-index> – A single controller IP address in the range 1-12.
	  • <IP> – A single IP address
	  • set-default – Default controller IP address

default-ap controller-ip [add <IP-list>| delete [<IP-index>|<IP>]| set-default]	Sets the default static controller IP address
	• controller-ip – Static controller IP address
	  • add – Adds a static controller IP address
	  • delete[<IP-index>|<IP>] – Deletes a static controller IP address
	  • <IP-index> – A single controller IP address
	  • <IP> – A single IP address
	  • set-default – Sets a default controller IP address

Example

```
RFController(config-wireless)#ap-ip 1 static-ip 192.168.10.25/24 192.168.10.1
RFController(config-wireless)#

RFController(config-wireless)#ap-ip 1 controller-ip add 192.168.10.25
10.10.1.4
```

```
RFController(config-wireless)#

RFController(config-wireless)#ap-ip default-ap controller-ip set-default
RFController(config-wireless)#
```

ap-standby-attempts-threshold

Wireless configuration commands

Sets the number of attempts after which the standby controller starts adopting APs.

Supported in the following platforms:

- Mobility RFS4000 Controller
- Mobility RFS6000 Controller
- Mobility RFS7000 Controller

Syntax

```
ap-standby-attempts-threshold <attempts>
```

Parameters

<attempts>	Sets the number of attempts to <attempts> in the range 5–200.

Example

```
RFController(config-wireless)#ap-standby-attempts-threshold 100
RFController(config-wireless)#
```

ap-timeout

Wireless configuration commands

Changes the default inactivity timeout for access points

Supported in the following platforms:

- Mobility RFS4000 Controller
- Mobility RFS6000 Controller
- Mobility RFS7000 Controller

Syntax

```
ap-timeout <index> <timeout>
```

Parameters

<index> <timeout>	• <index> – Access-points identified by a single index or by a list of indices. Use show wireless ap to view the AP's index or MAC address • <timeout> – Sets the new inactivity timeout (in seconds) to a value between 40 and 180.

Example

```
RFController(config-wireless)#ap-timeout 1 40
RFController(config-wireless)#
```

ap-udp-port

Wireless configuration commands

Configures the UDP port for layer 3 adoption of APs

You also need to configure the DHCP server providing the APs the same parameter.

Supported in the following platforms:

- Mobility RFS4000 Controller
- Mobility RFS6000 Controller
- Mobility RFS7000 Controller

Syntax

```
ap-udp-port <port>
```

Parameters

<port>	Sets the port number for layer 3 adoption of APs. <port> is a value in the range 1-65535.

Example

```
RFController(config-wireless)#ap-udp-port 20
RFController(config-wireless)#
```

auto-select-channels

Wireless configuration commands

Specifies a list of channels that will be used when *automatic channel scan* (ACS) and *dynamic frequency selection* (DFS)

Supported in the following platforms:

- Mobility RFS4000 Controller
- Mobility RFS6000 Controller
- Mobility RFS7000 Controller

Syntax

```
auto-select-channels [11a|11bg] [<channel-list>|
       add <channel-list>|remove <channel-list>]
```

Parameters

[11a|11bg] [<channel-list>| add <channel-list>| remove <channel-list>]	A comma separated list of 802.11a or 802.11bg channels • <channel-list> – a list of comma separated channels • add <channel-list> – adds <channel-list> channels to existing list • remove <channel-list>– remove <channel-list> channels from existing list

Example

```
RFController(config-wireless)#auto-select-channels 11a 1,3,5
RFController(config-wireless)#
```

broadcast-tx-speed

Wireless configuration commands

Configure the rate at which broadcast and multicast traffic is transmitted between the controller and wireless client

Supported in the following platforms:

- Mobility RFS4000 Controller
- Mobility RFS6000 Controller
- Mobility RFS7000 Controller

Syntax

```
broadcast-tx-speed [range|throughput]
```

Parameters

range	Uses a lowest basic rate, but provides the maximum range (default)
throughput	Uses a highest basic rate, but provides the maximum throughput

Example

```
RFController(config-wireless)#broadcast-tx-speed range
RFController(config-wireless)#

RFController(config-wireless)#broadcast-tx-speed throughput
RFController(config-wireless)#
```

client

Wireless configuration commands

Use this command to configure a wireless client

This command creates an exclude-list or include list. Creating a list moves the user to a new mode `config-wireless-client-list`.

Refer section *config-wireless-client-list commands on page 613* for `(config-wireless-client-list)` command summary.

Supported in the following platforms:

- Mobility RFS4000 Controller
- Mobility RFS6000 Controller
- Mobility RFS7000 Controller

Syntax

```
client [exclude-list|include-list] <list-name>
```

Parameters

exclude-list <list-name>	Sets the wireless client exclude list configuration. A Client NAC check is conducted, except for those in the exclude list. Devices in the exclude list will not have a NAC check performed.
include-list <list-name>	Defines the wireless client include list configuration. No Client NAC check is conducted, except for those in the include list. Devices in the include-list will have NAC checks.
<list-name>	Name of the list to be created.

Example

```
RFController(config-wireless)#client exclude-list JustMe
RFController(config-wireless-client-list)#
```

Configuring a client

Refer to the configurations below to:

- Create an exclude list.

  RFController(config-wireless)#client exclude-list protected-hosts
  RFController(config-wireless-client-list)#

- Add a host entry into the exclude list.

  RFController(config-wireless-client-list)# station printers 00:00:AA:DD:EE:11/00:00:FF:DD:EE:11

  RFController(config-wireless-client-list)# station testing-host1 00:11:AA:03:1B:FE

- Associate the exclude list to a WLAN.

  ```
  RFController(config-wireless-client-list)# wlan 1
  ```

- Configure RADIUS server parameters.

```
RFController(config-wireless)# wlan 1 nac-server primary 192.168.0.1
RFController(config-wireless)# wlan 1 nac-server primary secret 0 testing
RFController(config-wireless)# wlan 1 nac-server secondary 192.168.1.1
RFController(config-wireless)# wlan 1 nac-server secondary secret 0 testing123
```

- Enable NAC for a WLAN.

```
RFController(config-wireless)# wlan 1 nac-mode do-nac-except-exclude-list
```

- Undo a configuration.

```
RFController(config-wireless)# client exclude-list protected-hosts
RFController(config-wireless-client-client)# no station testing-host1
RFController(config-wireless)# no client exclude-list protected-hosts
RFController(config-wireless)# no wlan 1 nac-server primary
RFController(config-wireless)# no wlan 1 nac-server primary secret
RFController(config-wireless)# no wlan 1 nac-server secondary
RFController(config-wireless)# no wlan 1 nac-server secondary
radius-key
RFController(config-wireless)# no wlan 1 nac exclude-list
protected-hosts
```

config-wireless-client-list commands

Use `(config-wireless)# client` to enter the (`config-wireless-client-list`) instance. Use this instance, to create an exclude list or include list.

This table summarizes `config-wireless-client-list` commands:

Command	Description
clrscr	Clears the display screen
end	Ends the current mode and moves to the EXEC mode
exit	Ends the current mode and moves to the previous mode
help	Displays the interactive help system
no	Negates a command or sets its defaults
service	Provides a means of troubleshooting and debugging
show	Displays running system information
station	Defines a Client's MAC configuration
wlan	Sets Wireless LAN related parameters

station

config-wireless-client-list commands

Adds a specified MAC entry into the client's exclude or include list

Syntax

```
config-wireless-client-list station <host-name> [<MAC>|
<MAC/Mask>]
```

Parameters

<host-name> [<MAC>|<MAC/Mask>]	Defines an index for this host entry in the client list. The host station name <host-name> must be of size 1-21 characters. • <MAC> –Sets the Client mac address in AA-BB-CC-DD-EE-FF or AA:BB:CC:DD:EE:FF or AABB.CCDD.EEFF format. • <MAC/Mask> – Sets the Client MAC address and mask in AA-BB-CC-DD-EE-FF or AA:BB:CC:DD:EE:FF or AABB.CCDD.EEFF format.

Example

```
RFController(config-wireless-client-list)#station ExcludeList1
AA:BB:CC:DD:EE:FF
RFController(config-wireless-client-list)#
```

wlan

config-wireless-client-list commands

Adds a client exclude list name into/from the WLAN

Syntax

```
wlan [<index>|<index-list>]
```

Parameters

wlan [<index>| <index-list>]	• <index> – Sets a single WLAN index in the range 1-256 • <index-list> – A list (1,3,7) or range (3-7) of WLAN indices

Example

```
RFController(config-wireless-client-list)#wlan 1
RFController(config-wireless-client-list)#
```

clrscr

Wireless configuration commands

Clears the display screen

Supported in the following platforms:

- Mobility RFS4000 Controller
- Mobility RFS6000 Controller
- Mobility RFS7000 Controller

Syntax

```
clrscr
```

Parameters

None

Example

```
RFController(config-wireless)#clrscr
RFController(config-wireless)#
```

cluster-master-support

Wireless configuration commands

Sets the parameters for cluster master support

This is required for cluster level functions.

Supported in the following platforms:

- Mobility RFS4000 Controller
- Mobility RFS6000 Controller
- Mobility RFS7000 Controller

Syntax

```
cluster-master-support enable
```

Parameters

enable	Enables the cluster master support. This is required for cluster level functions.

Usage Guidelines

Use the **{no} cluster-master-support enable** command to disable this feature. By default, it is disabled.

Example

```
RFController(config-wireless)#cluster-master-support enable
RFController(config-wireless)#
```

convert-ap

Wireless configuration commands

Changes the mode of operation of an AP to either sensor or standalone

Supported in the following platforms:

- Mobility RFS4000 Controller
- Mobility RFS6000 Controller
- Mobility RFS7000 Controller

NOTE
The number of APs supported by `convert-ap` command differs for each controller.
- Mobility RFS7000 Controller supports <1-256> APs
- Mobility RFS6000 Controller supports <1-64> APs
- Mobility RFS4000 Controller supports <1-6> APs

```
convert-ap <ap-index> [default|sensor|standalone]

convert-ap <ap-index> [default|standalone]
convert-ap <ap-index> sensor {static-ip <IP/Mask>
       {<gateway-IP>}}
```

Parameters

<ap-index> [default|sensor|standalone]	Sets the indices of the APs to be converted.
	• <ap-index> – The index of the AP to be converted. This index can be found from the 'show wireless ap' command.
	• default – Does not force conversion. Lets the AP negotiate its normal mode of operation with the controller.
	• sensor {static-ip <IP/Mask> {<gateway-IP>}}– Converts an BR300 to operate as an IPS (*Intrusion Prevention System*) sensor.
	  • static-ip <IP/Mask> – Optional. Sensor must use specific static IP address.
	  • <IP/Mask> – Sensor IP address and network mask.
	  • <gateway-IP> – Optional. Specify gateway IP address for sensors
	NOTE: The controller will not be able to adopt this AP again until it is converted back to a BR300 using the `sensor <1-256> revert-to-ap` command
	NOTE: The controller will not be able to adopt this AP again until the AP is converted back to a thin-AP using the AP's configuration interface.

Example

```
RFController(config-wireless)#convert-ap 1 default
```

Converting an AP to sensor

To convert a BR300 to a sensor:

1. Use `sensor` command to setup the sensor.

```
RFController(config-wireless)#sensor default-config ?
ip-mode         configure the IP address mode of the sensors
wips-server-ip  specify IP addresses of the WIPS server
Select either ip-mode or wips-server-ip as the sensor parameter.
```

2. Specify the VLAN over which the sensors are available. This will help the controller detect them.

```
RFController(config-wireless)#sensor vlan 10
```

3. Use `convert-ap` command to convert the selected AP into a sensor directly from the controller.

```
RFController(config-wireless)#convert-ap 1 sensor
```

NOTE
To convert multiple APs' to Sensor, do it one by one and do config modifications.

country-code

Wireless configuration commands

Sets the country of operation

All existing radio configurations will be erased

Supported in the following platforms:

- Mobility RFS4000 Controller
- Mobility RFS6000 Controller
- Mobility RFS7000 Controller

Syntax

```
country-code <country-code>
```

Parameters

<country-code>	Configures the controller to operate in a defined country. <country-code> is the 2 letter ISO-3166 country code.

Usage Guidelines

Use the `show wireless country code` command to view the list of supported countries

Example

```
RFController(config-wireless)#country-code ?
WORD  the 2 letter ISO-3166 country code ("show wireless country-code-list" to
see list of supported countries)

RFController(config-wireless)#country-code US
RFController(config-wireless)#
```

debug

Wireless configuration commands

Debugging functions for the controller (wireless)

Supported in the following platforms:

- Mobility RFS4000 Controller
- Mobility RFS6000 Controller
- Mobility RFS7000 Controller

Syntax

```
debug cc [access-point|all|alt|ap-containment|ap-detect|
capwap|cluster|config|dot11|eap|ids|kerberos|l3-mob|loc-ap|
loc-client|media|wireless-client|radio|radius|self-heal|smart|snmp|
system|wips|wisp|wlan] {debug|err|info|warn}
```

Parameters

access-point	Sets the parameters for the access-point logs
all	Sets the parameters for all the modules
alt	Sets the parameters for the address lookup logs
ap-containment	Sets the parameters for the ap-containment logs
ap-detect	Sets the parameters for the Rogue AP detection logs
capwap	Sets the parameters for the CAPWAP logs
cluster	Sets the parameters for the cluster related logs
config	Sets the parameters for the configuration change logs
dot11	Sets the parameters for the datapath logs
eap	Sets the parameters for the 802.11x eap logs
ids	Sets the parameters for the intrusion detection logs
kerberos	Sets the parameters for the kerberos logs
l3-mob	Sets the parameters for the Layer-3 mobility logs
loc-ap	Sets the parameters for the AP locationing logs
loc-client	Sets the parameters for the Client locationing logs
media	Sets the parameters for the encapsulation media logs
wireless-client	Sets the parameters for the wireless-client logs
radio	Sets the parameters for the radio logs
radius	Sets the parameters for the radius client logs
self-heal	Sets the parameters for the self healing logs
smart	Sets the parameters for the smart-rf logs
snmp	Sets the parameters for the snmp logs
system	Sets the parameters for the system call logs
wips	Sets the parameters for the WIPS sensor logs
wisp	Sets the parameters for the WISP logs
wlan	Sets the parameters for the WLan logs

For all the above parameters, the following optional values are set:

debug	all the messages are logged
err	only error and higher severity messages are logged
info	only information and higher severity messages are logged
warn	only warning and higher severity messages are logged

Example

```
RFController(config-wireless)#debug cc ?
access-point     access-point logs
all              all modules
alt              address lookup logs
```

```
ap-containment  rogue AP containment logs
ap-detect       rogue AP detection logs
capwap          capwap logs
cluster         cluster related logs
config          configuration change logs
dot11           datapath logs
eap             802.1x/eap logs
ids             intrusion detection logs
kerberos        kerberos logs
l3-mob          Layer3 mobility logs
loc-ap          loc-ap logs
loc-client          loc-Client logs
media           encapsulation media logs
wireless-client     wireless-client logs
radio           radio logs
radius          radius client logs
self-heal       Self Healing logs
smart           smart-rf logs
snmp            SNMP logs
system          system call logs
wips            WIPS sensor logs
wisp            WISP logs
wlan            wlan logs

RFController(config-wireless)#

RFController(config-wireless)#debug cc system warn
RFController(config-wireless)#debug cc l3-mob err
RFController(config-wireless)#debug cc config debug
RFController(config-wireless)#debug cc kerberos info
RFController(config-wireless)#
```

dhcp-one-portal-forward

Wireless configuration commands

Enables the option to forward DHCP responses to one portal when the destination wireless-client is known from the response content

Supported in the following platforms:

- Mobility RFS4000 Controller
- Mobility RFS6000 Controller
- Mobility RFS7000 Controller

Syntax

```
dhcp-one-portal-forward enable
```

Parameters

enable	Enables the option to forward DHCP responses to one portal when the destination wireless-client is known from the response content.

Usage Guidelines

Use the **{no} dhcp-one-portal-forward enable** command to disable forwarding DHCP responses.

Syntax

```
RFController(config-wireless)#dhcp-one-portal-forward enable
RFController(config-wireless)#
```

dhcp-sniff-state

Wireless configuration commands

Records wireless client DHCP state information

Supported in the following platforms:

- Mobility RFS4000 Controller
- Mobility RFS6000 Controller
- Mobility RFS7000 Controller

Syntax

```
dhcp-sniff-state enable
```

Parameters

enable	Allows support for recording DHCP state information for wireless clients

Use the **{no} dhcp-sniff-state enable** command to disable recording wireless client DHCP state information.

Example

```
RFController(config-wireless)#dhcp-sniff-state enable
RFController(config-wireless)#
```

dot11-shared-key-auth

Wireless configuration commands

Enables support for 802.11 shared key authentication

NOTE
Shared key authentication has known weaknesses that can compromise your WEP key. It should only be configured to accommodate wireless stations unable to carry out Open-System authentication.

Supported in the following platforms:

- Mobility RFS4000 Controller
- Mobility RFS6000 Controller
- Mobility RFS7000 Controller

Syntax

```
dot11-shared-key-auth enable
```

Parameters

enable	Enables support for shared key authentication

Usage Guidelines

Use the **{no} dot11-shared-key-auth enable** command to disable support for 802.11 shared key authentication.

Example

```
RFController(config-wireless)#dot11-shared-key-auth enable
RFController(config-wireless)#
```

end

Wireless configuration commands

Ends and exits the current mode and changes to the PRIV EXEC mode. The prompt changes to `RFController#`

Supported in the following platforms:

- Mobility RFS4000 Controller
- Mobility RFS6000 Controller
- Mobility RFS7000 Controller

Syntax

```
end
```

Parameters

None

Example

```
RFController(config-wireless)#end
RFController#
```

exit

Wireless configuration commands

Ends the current mode and moves to the previous mode (GLOBAL-CONFIG). The prompt changes to `RFController(config)#`

Supported in the following platforms:

- Mobility RFS4000 Controller
- Mobility RFS6000 Controller
- Mobility RFS7000 Controller

Syntax

```
exit
```

Parameters

None

Example

```
RFController(config-wireless)#exit
RFController(config)#
```

fix-broadcast-dhcp-rsp

Wireless configuration commands

Converts broadcast DHCP server responses to unicast

Supported in the following platforms:

- Mobility RFS4000 Controller
- Mobility RFS6000 Controller
- Mobility RFS7000 Controller

Syntax

```
fix-broadcast-dhcp-rsp enable
```

Parameters

enable	Enables support for converting broadcast DHCP server responses to unicast

Usage Guidelines

Use the **{no} fix-broadcast-dhcp-rsp enable** command to disable converting broadcast DHCP server responses to unicast.

Example

```
RFController(config-wireless)#fix-broadcast-dhcp-rsp enable
RFController(config-wireless)#
```

help

Wireless configuration commands

Displays the system's interactive help (in HTML format)

Supported in the following platforms:

- Mobility RFS4000 Controller
- Mobility RFS6000 Controller
- Mobility RFS7000 Controller

Syntax

```
help
```

Parameters

None

Example

```
RFController(config-wireless)#help
CLI provides advanced help feature.  When you need help,
anytime at the command line please press '?'.

If nothing matches, the help list will be empty and you must backup
until entering a '?' shows the available options.
Two styles of help are provided:
1. Full help is available when you are ready to enter a
   command argument (e.g. 'show ?') and describes each possible
   argument.
2. Partial help is provided when an abbreviated argument is entered
   and you want to know what arguments match the input
   (e.g. 'show ve?'.)
RFController(config-wireless)#
```

hotspot

Wireless configuration commands

Configures the WLAN hotspot configuration

This overrides or adds to the existing hotspot configuration on the WLAN.

Supported in the following platforms:

- Mobility RFS4000 Controller
- Mobility RFS6000 Controller
- Mobility RFS7000 Controller

Syntax

```
hotspot query <query-index> <WORD>
[ap-mac|mu-mac||ssid|mu-ip|controller-ip|controller-name|user-string]
```

Parameters

<query-index>	The index of this query in the query list. Can be in the range of 1 and 10.
<WORD> [controller-ip||ssid |mu-mac|mu-ip| controller-name| user-string]	The name of the field in the URL whose value is substitute with the parameters • ap-mac – AP MAC address of the MU. • controller-ip – The controller's router ip-address for the external hotspot server • mu-mac – MAC address of teh MU. • ssid – The WLAN's SSID • mu-ip – The MU's IP address • controller-name – The controller's name on the network • user-string – Specifies that the value of the query is a user string.

Example

```
RFController(config-wireless)# hotspot query 1 user-name user-string
RFController(config-wireless)# hotspot query 2 from client-ip
RFController(config-wireless)#
```

load-balance

Wireless configuration commands

Configures the user load balance mode

Supported in the following platforms:

- Mobility RFS4000 Controller
- Mobility RFS6000 Controller
- Mobility RFS7000 Controller

Syntax

```
load-balance [by-count|by-throughput]
```

Parameters

by-count	In load balance by user count, the load on the radio is measured by the number of clients associated. The desired balance is to have equal number of clients on the radios in the group. By default, the load balance is configured for *by-count* when the controller boots up with factory default configuration.
by-throughput	In load balance by radio throughput (threshold 1 Mbps) the load on the radio is measured by the current average throughput rate. The desired balance is to have similar wireless traffic on the radios in the group.

Example

```
RFController(config-wireless)#load-balance by-throughput
RFController(config-wireless)#
```

mac-auth-local

Wireless configuration commands

Configures the local MAC authentication list

Supported in the following platforms:

- Mobility RFS4000 Controller
- Mobility RFS6000 Controller
- Mobility RFS7000 Controller

Syntax

```
mac-auth-local <1-1000> [allow|deny|rate-limit]

mac-auth-local <1-1000> [allow|deny] <starting-MAC>
       <ending-MAC> [<list>|not-mapped] {<radio-desc>|
       zone [<1-48>|default|unknown]}

mac-auth-local <1-1000> rate-limit
[wired-to-wireless|wireless-to-wired] <100-1000000>
```

Parameters

<1-1000>	Sets the mac-auth-local entry index to a value between 1 and 1000.
allow	Allows wireless clients that match this rule to associate.
deny	Denies association to wireless clients that match this rule.
rate-limit	Sets the rate limit value for this ACL entry.
<starting-MAC>	Starting MAC address in AA-BB-CC-DD-EE-FF or AA:BB:CC:DD:EE:FF format.
<ending-MAC>	Ending MAC address in AA-BB-CC-DD-EE-FF or AA:BB:CC:DD:EE:FF format.
<list>	Configures the local MAC authentication list.Sets the list (1,3,7) or range (3-7) of WLAN indices.
not-mapped	An unmapped row in the ACL.
<radio-desc>	Optional radio description substring.
zone [<1-48>|default|unknown]	Optional GeoFencing location information for devices matching this ACL information. • <1-48> – Administrator defined-id. • default – The user has been located within the site in the default zone. • unknown – If the users location is currently unknown or out of bounds of the site.
rate-limit [wired-to-wireless|wireless-to-wired] <100-1000000>	Set the rate limit for ACL • wired-to-wireless – Sets rate for down link direction from network to. wireless client. • wireless-to-wired – Sets the rate for up link direction from wireless client to network. • <100-1000000> – The rate in kbps.

Example

```
RFController(config-wireless)#mac-auth-local 1 allow 01:02:03:04:05:06
01:02:03:04:05:07 not-mapped
RFController(config-wireless)#mac-auth-local 2 deny
01-20-30-40-50-60 01-20-30-40-50-70 not-mapped
RFController(config-wireless)#mac-auth-local 1 allow 01:02:03:04:05:06
01:02:03:04:05:07 not-mapped zone 1
```

manual-wlan-mapping

Wireless configuration commands

Manually maps WLANs configured on a radio

Supported in the following platforms:

- Mobility RFS4000 Controller
- Mobility RFS6000 Controller
- Mobility RFS7000 Controller

Syntax

```
manual-wlan-mapping enable
```

Parameters

enable	Enables support for manual WLAN mapping.

Usage Guidelines

Use the **{no} manual-wlan-mapping enable** command to disable manual mapping of WLANs configured on a radio.

Example

```
RFController(config-wireless)#manual-wlan-mapping enable
RFController(config-wireless)#
```

wireless-client

Wireless configuration commands

Configures wireless client related parameters

Supported in the following platforms:

- Mobility RFS4000 Controller
- Mobility RFS6000 Controller
- Mobility RFS7000 Controller

Syntax

```
wireless-client [association-history|probe-history]

wireless-client association-history [enable|clear]
wireless-client probe-history [enable|add <1-200> <MAC>]
```

Parameters

association-history [enable|clear]	Enables a wireless client's association history. • enable – Enables a wireless client's association history. • clear – Clears the association history for all wireless clients.

probe-history [enable|add <1-200> <MAC>	wireless client probe logging configuration commands.
	• enable – Enables a wireless client's probe logging feature.
	• add <1-200> <MAC>– Adds a wireless client to probe history logging.
	  • <1-200> – Select an index value between 1 and 200 to add probe logging MAC.
	  • <MAC> – Sets the MAC address of the mobile used for probe history logging

Example

```
RFController(config-wireless)#wireless-client probe-history enable
RFController(config-wireless)#wireless-client association-history enable
RFController(config-wireless)#wireless-client probe-history add 20
AA-BB-CC-DD-EE-FF
RFController(config-wireless)#
```

mobility

Wireless configuration commands

Sets mobility parameters

Supported in the following platforms:

- Mobility RFS4000 Controller
- Mobility RFS6000 Controller
- Mobility RFS7000 Controller

Syntax

```
mobility [enable|local-address|max-roam-period|peer]

mobility enable
mobility local-address <IP>
mobility max-roam-period <1-300>
mobililty peer <IP>
```

Parameters

enable	Enables mobility globally
local-address <ip>	Sets the local address for mobility • <IP> – IP address in A.B.C.D format
max-roam-period <1-300>	Sets the Max Roam Period for a wireless client (in seconds) to a value in the range of 1 and 300.
peer <ip>	Adds a peer to this mobility region • <IP> – IP address of the Peer in A.B.C.D format

Example

```
RFController(config-wireless)#mobility enable
RFController(config-wireless)#mobility local-address 12.12.12.1
RFController(config-wireless)#mobility max-roam-period 10
RFController(config-wireless)#mobility peer 157.208.235.108
RFController(config-wireless)#
```

multicast-packet-limit

Wireless configuration commands

Sets a multicast packet limit, per second, for a VLAN. This limits the broadcast/multicast packets per VLAN. The default value is 32 broadcast/multicast packets per second. Setting the limit to 0 disables this control.

Supported in the following platforms:

- Mobility RFS4000 Controller
- Mobility RFS6000 Controller
- Mobility RFS7000 Controller

Syntax

```
multicast-packet-limit <0-128> [<vlan-id>|<vlan-id-range>]
```

Parameters

<0-128>	Sets the multicast packet limit per second.
<vlan-id>	Defines the single VLAN ID in the range 1-4094 the new limit applies to.
<vlan-id-range>	Defines a list of VLAN IDs in the format 1,3,7 or range 3-7 of VLAN IDs

Example

```
RFController(config-wireless)#multicast-packet-limit 120 50
RFController(config-wireless)#

RFController(config-wireless)#multicast-packet-limit 120 1,10,25
RFController(config-wireless)#
```

multicast-throttle-watermark

Wireless configuration commands

Configures watermarks for supporting bursts of broadcast/multicast frames

Supported in the following platforms:

- Mobility RFS4000 Controller
- Mobility RFS6000 Controller
- Mobility RFS7000 Controller

Syntax

```
multicast-throttle-watermarks low <0-100> high <0-100>
```

Parameters

low <0-100>	Sets the low water-mark. If the percentage of free packets in the system is lower than this threshold, the incoming frame is dropped.
high <0-100>	Sets the high water-mark. If the percentage of free packets in the system is between the low water-mark and this value, the packet is subjected to a random-early-drop. If free packets are greater than this value, the packet is processed.

Example

```
RFController(config-wireless)#multicast-throttle-watermarks low 10 high 20
RFController(config-wireless)#
```

nas-id

Wireless configuration commands

Configures the NAS ID to be sent to the RADIUS server

Supported in the following platforms:

- Mobility RFS4000 Controller
- Mobility RFS6000 Controller
- Mobility RFS7000 Controller

Syntax

```
nas-id <nas-id>
```

To override nas-id on a per WLAN basis:

```
wlan <1-4098> nas-id <nas-id>
```

Parameters

<nas-id>	A character string to be used as the NAS ID. Can be up to 256 characters long.

Example

```
RFController(config-wireless)#nas-id WIRELESSWELL
RFController(config-wireless)#
RFController(config-wireless)#wlan 1 nas-id WIRELESSWELL1
```

nas-port-id

Wireless configuration commands

Configures the NAS port ID that must be sent to the RADIUS server

Supported in the following platforms:

- Mobility RFS4000 Controller
- Mobility RFS6000 Controller
- Mobility RFS7000 Controller

Syntax

```
nas-port-id <port-id>
```

Parameters

<port-id>	The port ID to be sent to the RADIUS server.

Example

```
RFController(config-wireless)#nas-port-id portWIRELESSWELL
RFController(config-wireless)#
```

no

Wireless configuration commands

Negates a command or sets its defaults. All the parameters mentioned in the syntax can be negated using the **no** command.

Supported in the following platforms:

- Mobility RFS4000 Controller
- Mobility RFS6000 Controller
- Mobility RFS7000 Controller

Syntax

```
no [aap|admission-control|adoption-pref-id|
adopt-unconf-radio|ap|ap-containment|ap-detection|ap-image|
ap-ip|ap-standby-attempts-threshold|ap-timeout|ap-udp-port|
auto-select-channel|broadcast-tx-speed|client|
cluster-master-support|country-code|debug|
dhcp-one-portal-forward|dhcp-sniff-state|
dot11-shared-key-auth|fix-broadcast-dhcp-rsp|hotspot|ids|
mac-auth-local|manual-wlan-mapping|wireless-client|mobility|
multicast-packet-limit|multicast-throttle-watermarks|nas-id|
nas-port-id|proxy-arp|qos-mapping|radio|rate-limit|
secure-wispe-default-secret|self-heal|sensor|service|show|
smart-rf|smart-scan-channels|wips|wlan|wlan-bw-allocation]
```

Parameters

Refer to the individual commands for the parameters negated using the **no** command.

Example

```
RFController(config-wireless)#no mobility enable
RFController(config-wireless)#
```

proxy-arp

Wireless configuration commands

Responds to ARP requests from the RON to the WLAN on behalf of wireless clients

Supported in the following platforms:

- Mobility RFS4000 Controller
- Mobility RFS6000 Controller
- Mobility RFS7000 Controller

Syntax

```
proxy-arp enable
```

Parameters

enable	Enables the support for proxy arp

Usage Guidelines

Use the **no proxy-arp** enable command to disable.

Example

```
RFController(config-wireless)#proxy-arp enable
RFController(config-wireless)#
```

qos-mapping

Wireless configuration commands

Configures QoS mappings between the wired and wireless domains

Supported in the following platforms:

- Mobility RFS4000 Controller
- Mobility RFS6000 Controller
- Mobility RFS7000 Controller

Syntax

```
qos-mapping [wired-to-wireless|wireless-to-wired]

qos-mapping wired-to-wireless [dot1p <0-7>|dscp <0-63>]
[<0-7>|tid0|tid1|tid2|tid3|tid4|tid5|tid6|tid7]

qos-mapping wireless-to-wired [tid0|tid1|tid2|tid3|tid4|tid5|tid6|tid7] dot1p
<0-7>
```

Parameters

wired-to-wireless [dot1p <0-7>|dscp <0-63>] [<0-7>|tid0|tid1|tid2|tid3 | tid4|tid5|tid6|tid7]	Mappings used while controlling wired traffic over the air . • dot1p <0-7> – Configures the mapping of 802.1p tags to access categories. You can specify more than one 802.1p tags with in the range 0 and 7. • dscp <0-63> – Configures the mapping of DSCP values to access categories. You can specify more than one DSCP values in the range 0-63. • tid0, tid3– best effort category traffic • tid1, tid2 – background category traffic • tid4, tid5 – video traffic category traffic • tid6, tid7 – voice traffic category traffic
wireless-to-wired [tid0|tid1|tid2|tid3| tid4|tid5|tid6|tid7] dot1p <0-7>	Mappings used while controlling wireless traffic to the wired side. • tid0, tid3– best effort category traffic • tid1, tid2 – background category traffic • tid4, tid5 – video traffic category traffic • tid6, tid7 – voice traffic category traffic • dot1p <0-7> – Configures the mapping of 802.1p tags to access categories. You can specify more than one 802.1p tags with in the range 0 and 7.

Example

```
RFController(config-wireless)#qos-mapping wireless-to-wired background dot1p 5
RFController(config-wireless)#
```

radio

Wireless configuration commands

Sets radio related parameters

Supported in the following platforms:

- Mobility RFS4000 Controller
- Mobility RFS6000 Controller
- Mobility RFS7000 Controller

NOTE
The radios `group-id` range differs from controller to controller.
- Mobility RFS7000 Controller – Supports a range between 0-255
- Mobility RFS6000 Controller – Supports a range between 0-64
- Mobility RFS4000 Controller – Supports a range between 1-6

Syntax

```
radio [<1-4096>/<radio-list>|add|all-11a|all-11an|all-11b|
          all-11bg|all-11bgn|antenna-mode|configure-8021X|
          default-11a|default-11an|default-11b|default-11bg|
          default-11bgn|dns-name]

radio [<1-4096>|<radio-list>|all-11a|all-11an|all-11b|
          all-11bg|all-11bgn|default-11a|default-11an|default-11b|
          default-11bg||default-11bgn] [admission-control|
          adoption-policy|adoption-pref-id|ampdu|amsdu|antenna-mode|
          base-bridge|beacon-interval|bridge-fwd-delay <4-30>|
          bridge-hello <1-10>|bridge-max-ageout <4-3600>|
          bridge-msg-age <6-40>|bridge-priority <0-65535>|bss|
          channel-power|client-bridge|copy-config-from|description|
          detector|dtim-period|dot11k|enforce-spec-mgmt|
          enhanced-beacon-table|enhanced-probe-table|
          group-id [<0-48>|<0-255>|<0-64>]|location-led|
          location-message|mac|max-clients|mesh-associations|
          moto-simple-voice enable|mu-power <0-20>|nas-id|
          nas-port-id|on-channel-scan|radio-number|
radar-test-mode|reset|reset-ap|
          |rf-mode|rss|rts-threshold|run-acs|
          self-heal-offset|short-gi|short-preamble|speed|timeout|
          tunnel|wmm]

radio <1-4096> admission control voice [max-mu <1-256>|
          max-perc <1-100>|max-roamed-mus <0-256>|
          res-roam-perc <0-100>]

radio <1-4096> adoption-policy [allow|deny]

radio <1-4096> adoption-pref-id <0-65535>

radio <1-4096> ampdu [min-spacing|rx-limit|tx-enable|
          tx-limit]
radio <1-4096> ampdu min-spacing [.25|.5|0|1|2|4|8]
radio <1-4096> ampdu rx-limit [16383|32767|65535|8191]
radio <1-4096> ampdu tx-enable
radio <1-4096> ampdu tx-limit <0-65535>
```

```
radio <1-4096> amsdu [rx-limit|tx-enable] [<3839>|<7935>]

radio <1-4096> antenna-mode [diversity|mimo|primary|
          secondary]

radio <1-4096> bss [<1-4>|add-wlans|auto]<wlan-list>
radio <1-4096> base-bridge [enable|max-clients <1-12>]
radio <1-4096> beacon-interval <50-200>
radio <1-4096> bridge-fwd-delay <4-30>
radio <1-4096> bridge-hello <1-10>
radio <1-4096> bridge-max-ageout <4-3600>
radio <1-4096> bridge-msg-age <6-40>
radio <1-4096> bridge-priority <0-65535>

radio <1-4096> channel-power [indoor|outdoor] [<1-200>|acs|
          random] <1-36> [20Mhz|40Mhz]
radio <1-4096> channel-power [indoor|outdoor] [<1-200>]
<1-36> [<lower|upper>]

radio <1-4096> client-bridge [enable|mesh-timeout <2-200>|
          ssid <SSID>]
radio <1-4096> client-bridge [bb-radio|bridge-select-mode]
radio <1-4096> client-bridge bb-radio <1-16> <radio-MAC>
radio <1-4096> client-bridge bridge-select-mode
          [auto|manual]
radio <1-4096> copy-config-from [<1-4096>|default-11a|
          default-11b|default-11bg]

radio <1-4096> description <description>
radio <1-4096> dtim-period <1-50> bss <1-4>
radio <1-4096> detector
radio <1-4096> dot11k [enable|quiet-element
{defaults|duration|enable}]
radio <1-4096> dot11k quiet-element duration <20-150> interval <200-255>
radio <1-4096> enforce-spec-mgmt enable
radio <1-4096> enhanced-beacon-table
radio <1-4096> enhanced-probe-table

radio <1-4096> group-id <1-256>

radio <1-4096> location-led [start-flashing|stop-flashing]
radio <1-4096> location-message <message>

radio <1-4096> mac <MAC>
radio <1-4096> max-clients <units>
radio <1-4096> mu-power <0-20>
radio <1-4096> moto-simple-voice enable

radio <1-4096> nas-id <nas-id>
radio <1-4096> nas-port-id <nas-port-id>

radio <1-4096> on-channel-scan

radio <1-4096> radio-number <0-2>
radio <1-4096> radar-test-mode enable
radio <1-4096> reset
radio <1-4096> reset-ap

radio <1-4096> rf-mode [a|an|b|bg|bgn|custom|g|n]
```

```
radio <1-4096> rss enable
radio <1-4096> rts-threshold <0-2346>
radio <1-4096> run-acs

radio <1-4096> self-heal-offset <0-30>
radio <1-4096> short-gi enable
radio <1-4096> short-preamble

radio <1-4096> speed [1|11|12|18|2|24|36|48|54|5p5|6|9|
          basic1|basic11|basic11a|basic11an|basic11b1|basic11b2|
          basic11bg|basic11bgn|basic11g|basic11gn|basic11n|
          basic12|basic18|basic2|basic24|basic36|basic48|basic54|
          basic5p5|basic6|basic9|default|range|throughput]

radio <1-4096> timeout <40-180>
radio <1-4096> tunnel tx-rate-class <1-4>

radio <1-4096> wmm [background|best-effort|video|voice]
          [aifsn <1-15>|burst <0-65535>|cw <0-15>]
All the above radio commands can be executed using <radio-list> also.
radio [all-11a|default-11a] [admission-control|
          adoption-policy|adoption-pref-id|antenna-mode|base-bridge|
          beacon-interval|bridge-fwd-delay|bridge-hello|
          bridge-max-ageout|bridge-msg-age|bridge-priority|bss|
          channel-power|client-bridge|detector|dtim-period|
          enforce-spec-mgmt|enhanced-beacon-table|
          enhanced-probe-table|location-led|
          location-message|max-clients|moto-simple-voice|
          mu-power|on-channel-scan|reset|reset-ap|
          rf-mode|rss|rts-threshold|run-acs|self-heal-offset|speed|
          wmm|tunnel]

radio [all-11an|default-11an] [adoption-policy|ampdu|
          antenna-mode|bss|channel-power|rf-mode|speed|tunnel|
          short-gi]

radio [all-11b|default-11b] [adoption-policy|
          antenna-mode|base-bridge|beacon-interval|bridge-fwd-delay|
          bridge-hello|bridge-max-ageout|bridge-msg-age|
          bridge-priority|bss|channel-power|client-bridge|detector|
          dtim-period|enhanced-beacon-table|enhanced-probe-table|
          location-message|max-clients|mu-power|
          on-channel-scan|reset|reset-ap|rf-mode|rss|
          rts-threshold|run-acs|self-heal-offset|speed|tunnel|
          short-preamble]

radio [all-11bg|default-11bg] [admission-control|
          adoption-policy|adoption-pref-idantenna-mode|base-bridge|
          beacon-interval|bridge-fwd-delay|bridge-hello|
          bridge-max-ageout|bridge-msg-age|bridge-priority|bss|
          channel-power|client-bridge|detector|dtim-period|
          enhanced-beacon-table|enhanced-probe-table|location-led
          location-message|max-clients|moto-simple-voice|
          mu-power|on-channel-scan|reset|reset-ap|
          rf-mode|rss|rts-threshold|run-acs|self-heal-offset|
          speed|tunnel|short-preamble|wmm]

radio [all-11bgn|default-11bgn] [adoption-policy|ampdu|
          antenna-mode|bss|channel-power|rf-mode|speed|tunnel|
          short-gi]
```

```
radio add <1-4096> <MAC> [11a|11an|11b|11bg|11bgn]
          {[aap5131|aap5181|ap300|ap650|aap7131|aap7181|ap100|ap4131]}

radio antenna-mode [diversity|mimo|primary|secondary]

radio configure-8021X <username> <password> {<MAC>}

radio dns-name <dns-name> {<MAC>}
radio lldp [hold-time|mode|refresh-interval]
radio lldp hold-time <4-10>
radio lldp mode disable
radio lldp refresh-interval <30-32768>
```

Parameters

<1-4096>	Defines a single radio index.
<radio-list>	Creates a list (1,3,7) or range (3-7) of radio indices.
add <1-4096> <MAC> [11a|11an|11b|11bg|11bgn] [*br5181|br300|br7131]}*	Adds the specified radio to the radio list at index specified for the value in the range 1-4096. • [11a|11an|11b|11bg|11bgn] – The radio type • [br5181|br300|br7131] – Optional. The radio model. The options available will depend on the radio type selected.
all-11a	All 11a radios currently in configuration
all-11an	All 11an radios currently in configuration
all-11b	All 11b radios currently in configuration
all-11bg	All 11bg radios currently in configuration
all-11bgn	All 11bgn radios currently in configuration
antenna-mode [diversity|mimo|primary|secondary]	Antenna diversity mode. Select diversity from: • diversity – Use full diversity (both antennas) • mimo – use MIMO • primary – Use primary antenna only • secondary – Use secondary antenna only
configure-8021X	Configures the 802.1X username and password on adopted access points
default-11a	Adopts the default 11a configuration template
default-11an	Adopts the default 11an configuration template
default-11b	Adopts the default 11b configuration template
default-11bg	Adopts the default 11bg configuration template
default-11bgn	Adopts the default 11bgn configuration template
dns-name <WORD> <AA-BB-CC-DD-EE-FF>	Configures dns-name to be used in L3-Discovery on adopted access-points. • <WORD> - Specify the dns-name the access-ports must use (upto 127 characters) • <AA-BB-CC-DD-EE-FF> - Change the dns-name only on the access-point with a specified MAC address. If not specified, the dns-name update is sent to all currently adopted access-points

lldp [hold-time|mode|refresh-interval]	Displays the commands related to LLDP advertisements.
	• hold-time <4-10>– Sets the HoldTime Multiplier value on LCAP. The default value is 4.
	  • <4-10> – Specifies the range of the HoldTime Multiplier value in seconds.
	• mode – Sets the LLDP status on LCAP.
	  • disable – Disables the LLDP advertisements.
	• refresh-interval <30-32768> – Sets the LLDP refresh interval on LCAP. This parameter indicates the interval at which LLDP frames are transmitted on behalf of the LLDP agent.
	  • <30-32768> – Specifies the range of Refresh Interval Value in seconds.
	NOTE: By default, the LLDP mode is disabled.

The following is the list of parameters for the **`radio <1-4096>, radio [all-11a|all-11an|all-11b|all-11bg|all-11bgn|default-11a||default-11an|default-11b|default-11bg|default-11bgn]`** commands.

admission-control voice [max-clients <0-256>| max-perc <0-100>| max-roamed-clients <0-256>| res-roam-perc <0-100>]	Sets the admission control parameters for voice. The following options are configured: • max-clients <0-256> – Configure the maximum number of clients to be admitted. • max-perc <0-100> – Configure the maximum percentage of air time allotted to voice traffic. • max-roamed-clients <0-256> – Configure the maximum number of roamed clients to be admitted. • res-roam-perc <0-100> –Configure the maximum percentage of air time exclusively allotted to clients that have roamed. This value is calculated relative to the max-perc value.
adoption-pref-id <0-65535>	Employs a preference identifier for this radio port. The radio port is more likely to be adopted by a wireless controller that is a preferred controller.
adoption-policy [allow|deny]	Specifies adoption policy. Select from : • allow – Allows adoption • deny – Denies adoption
ampdu [min-spacing [.25|.5|0|1|2|4|8]| rx-limit [16383|32767| 65535|8191]| tx-limit <0-65535>| tx-enable *{min-spacing [.25|.5|0|1|2|4|8]| rx-limit [16383|32767| 65535|8191]| tx-limit <0-65535>}*	Specifies the settings for the MAC Protocol frames. The following properties are configured: • min-spacing [.25|.5|0|1|2|4|8] – The spacing between MPDUs received in microseconds. • rx-limit [8191|16283|32767|65535] – The receive buffer limit in bytes. • tx-limit <0-65535> – The transmit buffer limit in bytes. • tx-enable {min-spacing [.25|.5|0|1|2|4|8]|rx-limit [16383|32767|65535|8191]|tx-limit <0-65535>} – Optional parameters for enabling transmitting A-MPDUs.
amsdu [rx-limit| tx-enable]	Specifies the settings for the MAC Service frames. The following properties are configured: • rx-limit – The receive buffer limit in bytes • tx-enable – Optional parameters for enabling transmitting A-MSDUs • <3839 bytes>|<7935 bytes> – The number of bytes received **NOTE:** Before executing this command, ensure the radio is present and is a BR650 model.
antenna-mode [diversity|mimo|primary|secondary]	Defines the antenna diversity mode. Select from the following options: • diversity–Full diversity (both antennas) • mimo – MIMO • primary–Primary antenna only • secondary–Secondary antenna only **NOTE:** Before executing this command, ensure the radio is present and is a BR300 model.

base-bridge [enable| max-clients <1-12>]	Sets base bridge values • enable – Allows the given radio to act as a base bridge and accept connections from client bridges. • max-clients <1-12> – Configures a base-bridge. Enter maximum client bridges allowed.
beacon-interval <50-200>	Sets the beacon interval (in K-uSec)
bridge-fwd-delay <4-30>	Sets the STP bridge forward delay (in seconds) • <4-30> - Time in seconds
bridge-hello <1-10>	Sets the STP bridge hello (in seconds) • <1-10> - Time in seconds
bridge-max-ageout <4-3600>	Sets the STP bridge maximum ageout (in seconds) • <4-3600> - Time in seconds
bridge-msg-age <6-40>	Sets the STP bridge message age (in seconds) • <6-40> - Time in seconds
bridge-priority <0-65535>	Sets the STP bridge priority (in seconds) • <0-65535> - Priority value
bss [<1-4>|add-wlans| auto] <wlans>	Maps WLANs to radio BSSIDs • <1-4>– Sets the BSS where WLANs are mapped • add-wlans <wlans> – Adds new WLANs to existing radios. The other WLANs on the radios are left as is. • auto <wlans> – Sets the automatic assignment of a BSS. The user selects WLANs, and the system assigns them to a BSS automatically. • <wlans> – Defines a list (1,3,7) or range (3-7) of WLAN indices. When a BSS is also specified, the first WLAN is used as the primary WLAN. When the auto option is used, the system automatically assigns the first four WLANs as primaries on their respective BSSIDs.

channel-power
[indoor|outdoor]
[<1-200>|acs|random]
	Sets the location, channel and transmit power level
	• indoor [<1-200>|acs|random]– Defines an indoor location
	  • <1-200> <4-20> {[lower|upper]} – Defines the channel number
	  • <4-20> – Power in dBm
	  • lower – Lower channel width mode
	  • upper – Upper channel width mode
	• outdoor [<1-200>|acs|random]– Defines an outdoor location
	  • <1-200> – Sets the channel number
	  • <4-20> – Sets the power in dBm
	  • acs <4-20> {[20 MHz | 40 Mhz]} – Enables ACS (*auto channel selection*). A radio will scan for the least congested channel at startup or controller reconfiguration.
	  • random <4-20> {[20 MHz | 40 Mhz]} – Random channel selection

client-bridge [bb-radio| bridge-selectmode| enable| mesh-timeout <2-200>| ssid <SSID>]	Defines client bridge settings.
	• bb-radio <1-16> <MAC>– add the preferred base bridge details.
	  • <1-16> – Enables the capability
	  • MAC – MAC address in AA-BB-CC-DD-EE-FF format
	• bride-select-mode [auto|manual]– Base bridge selection mode
	  • auto – Automatically select base bridge
	  • manual – Manually select base bridge
	• enable – Enables client-bridge functionality on radio
	• mesh-timeout [0|1|<2-200>] – Sets the client bridge link timeout.
	  • 0 – Disable uplink detection
	  • 1 – Uplink detect - shutdown when all mesh-backhaul links are down
	  • <2-200> – Timeout in seconds.
	• ssid <SSID> – Defines the ESSID of the WLAN

copy-config-from [<1-4096>|default-11a| default-11b| default-11bg|]	Copies the configuration from a previously configured radio. • <1-4096> – Defines a single radio index • default-11a – Uses the default 11a configuration template. • default-11b – Uses the default 11b configuration template. • default-11bg – Uses the default 11bg configuration template.
description <description>	Defines a description for this radio. <description> is a 20 character string.
detector	Dedicates this radio as a detector. No wireless clients can associate to a detector.

dot11k [enable| quiet-element {default|duration <20-150>|enable}]	Displays dot11k related commands.
	• enable – Enables 802.11k for the radio
	• quiet-element {default|duration|enable} – Displays quiet element configuration
	  • default – Setting it to defaults
	  • duration <20-150> – Time to remain quiet in TUs
	  • <20-150> {interval} – Range of Quiet duration in K-u seconds
	  • interval <200-255> – Displays the interval time in which quiet element is sent after specified number of Beacons
	  • <200-255> – Range of quiet interval
	  • enable – Enables the Quiet Element

dtim-period<1-50> *{bss <1-4>}*	Set the DTIM period (number of beacons between successive DTIMs). • <1-50> – Sets the DTIM period • bss <1-4>– Optional BSS index
enforce-spec-mgmt enable	Enforces spectrum management checks on specified radios. Only wireless clients that advertise spectrum management capabilities will be allowed to associate on this radio.
enhanced-beacon-table	Enables the enhanced beacon table for AP locationing.
enhanced-probe-table	Enables the enhanced probe table for Client locationing.

group-id <1-256>	Specifies the radio groups to balance user load. • For Mobility RFS7000 Controller, <0-255> – Radio group identifier used for an access-point, 0 disables the grouping. • For Mobility RFS6000 Controller, <0-64> – Radio group identifier used for an access-point, 0 disables the grouping.
location-led [start-flashing| stop-flashing]	Changes the mode of operation of the LEDs on an AP. • start-flashing – Requests parent-ap of specified radio to begin flashing its LEDs to help locate it. • stop-flashing – Requests parent-ap of specified radio to revert its LEDs to normal mode of operation.
location-message <message>	Specifies a message sent to all wireless clients that associate with these radios. This message <message> should not exceed 80 characters.
mac <MAC>	Changes the parent (access-point) MAC address of the radio.
max-wireless-clients <1-256>	Maximum number of wireless clients allowed to associate.
mesh-associations <1-3>	Displays Client bridge mesh associations • <1-3> – Displays number of mesh assocations
client-power <0-20>	Power adjustment level for wireless clients associated with this access-point. clients that support this element will reduce their transmit power by the specified value. • <0-20> – Power adjustment level in dBm.
nas-id <ID>	Configures a NAS ID for this radio. <ID> can be up to 256 characters long.
nas-port-id <ID>	Configures a NAS port id for this radio. <ID> can be up to 256 characters long.
on-channel-scan	Enables rogue scanning on this radio.
radio-number <0-2>	Enter the radio number only if there are two similar radios on the AP. Enter 0 (zero) or omit when there is no ambiguity.
radar-test-mode enable	Enables the radar test mode.
reset	Resets a radio (this will only reset the specified radio, not the complete access point).
reset-ap	Resets the parent AP (this will reset all radios on that access point).
rf-mode [a|an|b|bg|bgn| custom|g|n]	Selects the radio speed based on the radio mode selected.
rss enable	*Remote Site Survivability* (RSS) enables the delivery of secure uninterrupted wireless service in remote locations in the event of a device failure.
rts-threshold <0-2347>	Defines the RTS threshold in bytes.
run-acs	Runs an auto-channel-selection on a radio. The radio should already have been configured for ACS support.
self-heal-offset <0-30>	Configures the self-healing offset (measured in dBm), for regulatory compliance. **NOTE:** The offset is based off the regulatory maximum power for the specified channel ("show wireless regulatory" displays the max power allowed).

short-gi enable	Enables the Short GI value for both the 20 MHz and the 40 MHz channels for the 11n radio.
short-preamble	Enables support for the short preamble. **NOTE:** This disables support for long preamble. Mobiles that only support long preamble will not be able to associate.
speed [1|11|12|18|2|24|36|48|54|5p5|6|9|basic1|basic11|basic11a|basic11an|basic11b1|basic11b2|basic11bg|basic11bgn|basic11g|basic11gn|basic11n|basic12|basic18|basic2|basic24|basic36|basic48|basic54|basic5p5|basic6|basic9|range|throughput|default]	Configures the basic and supported data rates/speed • 1 1-Mbps • 11 11-Mbps • 12 12-Mbps • 18 18-Mbps • 2 2-Mbps • 24 24-Mbps • 36 36-Mbps • 48 48-Mbps • 54 54-Mbps • 5p5 5.5-Mbps • 6 6-Mbps • 9 9-Mbps • basic1 basic 1-Mbps • basic11 basic 11-Mbps • basic11a rate set (6,12,24 Mbps) • basic11an rate set (6,12,24, MCS 0-7) • basic11b1 rate set (1 and 2 Mbps) • basic11b2 rate set (1,2,5.5,11 Mbps) • basic11bg rate set (1,2,5.5,11,6,12,24 Mbps) • basic11bgn rate set (1,2,5.5,11,6,12,24, MCS 0-7) • basic11g rate set (6,12,24 Mbps) • basic11gn rate set (6,12,24, MCS 0-7) • basic11n rate set (MCS 0-7) • basic12 basic 12-Mbps • basic18 basic 18-Mbps • basic2 basic 2-Mbps • basic24 basic 24-Mbps • basic36 basic 36-Mbps • basic48 basic 48-Mbps

	• basic54 basic 54-Mbps
	• basic5p5 basic 5.5-Mbps
	• basic6 basic 6-Mbps
	• basic9 basic 9-Mbps
	• default {mcs <msc-range>} – Factory default rates based on radio-type.
	• throughput {mcs <msc-range>} – All rates basic (only 802.11g clients are allowed on 802.11bg radios).
	• range {mcs <msc-range>} – all rates enabled, the lowest one set to basic
	  • mcs – Configure the mcs rates / speed
	  • MCS – A list or range (eg: 0-5, 10,15) of MCS rates (0 to 15)

timeout <40-180>	The time out value in seconds for the selected radio.

tunnel tx-rate-class <1-4>	The tunnel transmit rate class for the radio. Select a value from 1 to 4.
wmm [background|best-effort|video|voice] [aifsn<1-15>|burst <0-65535>| cw<0-15>] wmm [video|voice] acm [enable|max-clients <1-64>]	Sets *802.11e/Wireless Multi Media* (WMM) parameters (supported only on BR300). • background – Prioritizes Background category traffic. • best-effort– Prioritizes Best Effort category traffic. • video – Prioritizes Video category traffic. • voice – Prioritizes Voice category traffic. • acm [enable|max-clients <1-64>] – Admission control parameters. Use `enable` to allow admission control.Enabling ACM on video enables ACM on the Voice access category. Use `max-clients` to specify the number of wireless clients that are allowed access on the specified categories. • aifsn <1-15> – *Arbitration Inter Frame Spacing Number* (AIFSN) defines the wait time (in milliSeconds) between data frames. Derived using AIFSN and the slot-time. • burst <0-65535> – Transmit-opportunity. Sets an interval when a particular WMM STA has the right to initiate transmissions onto the wireless medium. • cw <0-15> – *Contention Window* (cw) parameters. Wireless stations pick a number between 0 and the minimum contention window to wait before re-trying transmissions. Stations then double their wait time on a collision, until it reaches the maximum contention window.

Example

```
RFController(config-wireless)#radio 250 bss auto 3-5
RFController(config-wireless)#

RFController(config-wireless)#radio 1 amsdu tx-enable rx-limit 3839
RFController(config-wireless)#RFController
```

rate-limit

Wireless configuration commands

Sets the default rate limit per user in kbps, and applies to all enabled WLANs

Supported in the following platforms:

- Mobility RFS4000 Controller
- Mobility RFS6000 Controller
- Mobility RFS7000 Controller

Syntax

```
rate-limit [wired-to-wireless|wireless-to-wired] <0-100000>
```

Parameters

wired-to-wireless <100-100000>	Down link direction from network to wireless client • <100-100000> – rate in the range of <100-100000> kbps
wireless-to-wired <100-100000>	Up link direction from wireless client to network • <100-100000> – rate in the range of <100-100000> kbps

Usage Guidelines

Use **{no} rate-limit [wired-to-wireless|wireless-to-wired]** to remove the rate limit applied to the group

Example

```
RFController(config-wireless)#rate-limit wired-to-wireless 1000
RFController(config-wireless)#

RFController(config-wireless)#rate-limit wireless-to-wired 20000
RFController(config-wireless)#
```

secure-wispe-default-secret

Wireless configuration commands

Configures the default shared secret for secure WISPE

If a new shared secret is not configured for an AP or a list of APs, then a default shared secret will be assigned. The value of default shared secret is the string "default".

Supported in the following platforms:

- Mobility RFS4000 Controller
- Mobility RFS6000 Controller
- Mobility RFS7000 Controller

Syntax

```
secure-wispe-default-secret [<secret-key>|0 <secret-key>|
       2 <secret-key>]
```

Parameters

[<secret-key>| 0 <secret-key>| 2 <secret-key>]	Enter a secret key. The string length must not exceed 64 characters. • 0 <secret-key> – Password is specified unencrypted. • 2 <secret-key>– Password is specified encrypted with password-encryption secret. • <secret-key> – 8 to 64 characters.

Example

```
RFController(config-wireless)#secure-wispe-default-secret
0x1d8e4fc780be92537109
RFController(config-wireless)#
```

self-heal

Wireless configuration commands

Configures self healing values

Supported in the following platforms:

- Mobility RFS4000 Controller
- Mobility RFS6000 Controller
- Mobility RFS7000 Controller

Syntax

```
self-heal [interference-avoidance|neighbor-recovery]

self-heal interference-avoidance [enable|hold-time
<30-65535>|retries <0.0-15.0>]

self-heal neighbor-recovery [action|enable|neighbors|
run-neighbor-detect]
self-heal neighbor-recovery action [both|none|open-rates|
raise-power] radio [<1-4096>|<radio-list>]
self-heal neighbor-recovery neighbors <1-4096> [<1-4096>|
<radio-list>]
self-heal neighbor-recovery run-neighbor-detect
```

Parameters

interference-avoidance	Interference avoidance configuration.
enable	Enables/disables interference avoidance.
hold-time <30-65535>	The number of seconds to disable interference avoidance after a detection. This prevents a radio from changing channels continuously. Set the hold-time between 30-65535 seconds.
retries <0.0-15.0>	Defines the average number retries (0-15) causing a radio to re-run auto channel selection.
neighbor-recovery	Invokes neighbor recovery configuration commands.

action [both|none|open-rates|raise-power] radio [<1-4096>|<radio-list>]	Defines the radio's self healing action when neighbors are detected as down.
	• both – Raises the power to max and open all rates.
	• none – No action taken.
	• open-rates – Opens all rates.
	• raise-power – Raises the power to maximum.
	• radio [<1-4096>|<radio-list>] – Modifies the action for specified radio(s).
	  • <1-4096> – Sets a single radio index.
	  • <radio-list> – Defines a list (1,3,7) or range (3-7) of radio indices.

enable	Monitors access points and attempts to increase coverage on a detected failure.
neighbors <1-4096> [<1-4096>|<radio-index>]	Adds a radio as a neighbor. • <1-4096> – Sets a single radio index. • <radio-list> – Defines a list (1,3,7) or range (3-7) of radio indices.
run-neighbor-detect	Disassociates all wireless clients, clears current neighbors and runs neighbor detection again.

Example

```
RFController(config-wireless)#self-heal interference-avoidance enable
RFController(config-wireless)#self-heal interference-avoidance hold-time 600
RFController(config-wireless)#self-heal neighbor-recovery enable
Note: reducing the configured transmit power of radios will ensure that there
is room to increase power when a neighbor fails
RFController(config-wireless)#self-heal neighbor-recovery neighbors 1 1
RFController(config-wireless)#
```

sensor

Wireless configuration commands

Configures *Wireless Intrusion Protection System* (WIPS) parameters

Supported in the following platforms:

- Mobility RFS4000 Controller
- Mobility RFS6000 Controller
- Mobility RFS7000 Controller

Syntax

```
sensor [<1-48>|default-config|ping-interval|vlan]
sensor <1-48> [default-config|request-config|revert-to-ap]

sensor default-config [gateway-ip|ip-mode|wips-server-ip]
sensor default-config gateway-ip <IP>
sensor default-config ip-mode [dhcp|static <IP/Mask>]
sensor default-config wips-server-ip [primary|secondary]
       <IP>
sensor ping-interval <2-60>
sensor vlan <1-4094> {<1-4094>}
```

Parameters

<1-48> [default-config| requestconfig| revert-to-ap]	Select a sensor to reset/revert the AP to its original state. Use the **show wireless sensor** command to view the sensor index. • default-config – Restores the internal configuration of the sensor to default values. This sends the configuration to the sensor. • request-config – Polls the sensor for its latest configuration. • revert-to-ap – Reverts an IDS sensor back to an access point that can service wireless-clients.

default-config [gateway-ip|ip-mode| wips-server-ip]	Invokes the default configuration sent to sensors when configured.
	• gateway-ip <IP> – Configure the gateway IP address for sensors to <IP>.
	• ip-mode [dhcp|static <IP/Mask>] – Configures the IP address of the sensors.
	  • dhcp – Sensors use DHCP to obtain an IP address.
	  • static <IP/Mask> – Sensors use the specific static IP address.
	  • <IP/Mask> – Sets the sensor IP address and network mask.
	• wips-server-ip [primary|secondary] <IP> – Specifies the IP addresses of the WIPS server.
	  • primary <IP> – Specifies the primary IP address of the WIPS server.
	  • secondary <IP> – Specifies the secondary IP address of the WIPS server.

ping-interval <2-60>	Sets the ping interval (in seconds) between successive pings to sensors on the network.
vlan <1-4094>	Configures VLANs where sensors are discovered. • <1-4094> – Vlan IDs

Example

```
RFController(config-wireless)#sensor vlan 268 500
RFController(config-wireless)#
```

service

Wireless configuration commands

Invokes service commands to troubleshoot or debug `(config-wireless)` instance configurations

For more information, see "service" on page 37.

Supported in the following platforms:

- Mobility RFS4000 Controller
- Mobility RFS6000 Controller
- Mobility RFS7000 Controller

Syntax

```
service [clear|show|smart-rf|wireless]

service clear wireless wireless-client association-statistics

service show [cli|radio-neighbor|smart-rf|wireless]
service show cli

service show cli radio-neighbor mu <MAC>
service show smart-rf [debug-config|sensitivity]
service show smart-rf debug-config
service show smart-rf sensitivity [client|pattern|rates]
service show smart-rf sensitivity client {[<0-8192>|<MAC>]}
service show smart-rf sensitivity pattern [pattern-11a|
       pattern-11b|pattern-11bg|pattern-2-mbps]
service show smart-rf sensitivity rates <rate-flag>

service show wireless [ap-history|buffer-counters|
       enhanced-beacon-table|enhanced-probe-table|group|
       group-stats|legacy-load-balance|client-cache-buckets|
       client-cache-entry|mvlan|radio|radio-cache-entry|
       radio-hash-buckets|snmp-trap-throttle|vlan-cache-buckets|
       vlan-cache-entry|waiting]
service show wireless [buffer-counters|group-stats|
       legacy-load-balance|client-cache-buckets|radio-hash-buckets|
       snmp-trap-throttle|vlan-cache-buckets]

service show wireless ap-history {<MAC>}
service show wireless enhanced-beacon-table [config|report]
service show wireless enhanced-probe-table [config|report]
service show wireless group <1-256>
service show wireless client-cache-entry {[<1-8192>|<MAC>]}
service show wireless mvlan <1-256>
service show wireless radio {[<1-4094>|description|mapping]}
service show wireless radio-cache-entry {<MAC>}
service show wireless vlan-cache-entry {[<1-8192>|<MAC>]}
service show wireless waiting {<0-99> {<0-99>}}

service smart-rf [clear-history|load-from-file|replay|
       rescue|restore|save-to-file|simulate]
service smart-rf [clear-history|load-from-file|save-to-file]
service smart-rf replay enable
service smart-rf rescue [<MAC>|<1-4094>|<index-list>]
service smart-rf restore [<MAC>|<1-4094>|<index-list>]
```

```
service smart-rf simulate [coverage-hole|interference]
service smart-rf simulate coverage-hole <1-4096>
       <experienced-range> [<transmit-rate>|pattern-11a|
       pattern-11b|pattern-11bgn|pattern-2-mbps]
service smart-rf simulate interference [<MAC>|<1-4094>|
       <index-list>]

service wireless [ap-history|clear-ap-log|custom-cli|dot11i|
       dump-core|enhanced-beacon-table|enhanced-probe-table|
       free-packet-watermark|idle-radio-send-multicast|
       legacy-load-balance|map-radios|radio-misc-cfg|
       rate-scale|request-ap-log|save-ap-log|snmp-trap-throttle|
       sync-radio-entries|vlan-cache]
service wireless ap-history [clear|enable]
service wireless clear-ap-log {<ap-index>}
service wireless custom-cli [sh-wi-wireless-client|sh-wi-radio]
service wireless custom-cli sh-wi-wireless-client [ap-locn|
       ap-name|channel|dot11-type|ip|last-heard|mac|radio-bss|
       radio-desc|radio-id|ssid|state|vlan|wlan-desc|wlan-id|
       username]
service wireless custom-cli sh-wi-radio [adopt-info|
       ap-locn|ap-mac|ap-name|bss|channel|dot11-type|num-client|
       power|radio-desc|radio-id|state]

service wireless dot11i enforce pmkid-validation

service wireless enhanced-beacon-table [channel-set|enable|
       erase-report|max-ap|scan-interval|scan-time]
service wireless enhanced-beacon-table [enable|erase-report]
service wireless enhanced-beacon-table channel-set
       [a|an|bg|bgn] <1-200>
service wireless enhanced-beacon-table max-ap <0-512>
service wireless enhanced-beacon-table scan-interval <10-60>
service wireless enhanced-beacon-table scan-time <100-1000>

service wireless enhanced-probe-table [enable|erase-report|
       max-client|preferred|window-time]
service wireless enhanced-probe-table [enable|erase-report]
service wireless enhanced-probe-table max-client <0-512>
service wireless enhanced-probe-table preferred <MAC>
service wireless enhanced-probe-table window-time <10-60>

service wireless free-packet-watermark <0-100>
service wireless idle-radio-send-multicast enable
service wireless map-radios <1-127>
service wireless radio-misc-cfg <hex-mask>
service wireless request-ap-log <ap-index>
service wireless snmp-trap-throttle <1-20>
service wireless vlan-cache enable
```

Parameters

clear wireless wireless-client association-statistics	Clears statistics for wireless wireless client associations and dis-associations.

show [radio-neighbor|cli|smart-rf|wireless]	Displays the current running system information for this mode.
	• cli – Shows the CLI commands available in this mode.
	• radio-neighbor mu <MAC> – Displays neighboring radios for a station
	  • mu – Specify the MAC address of the MU.
	  • <MAC> – Displays MAC address in AA-BB-CC-DD-EE-FF format
	• smart-rf [debug-config|sensitivity] – Displays smart-rf management commands.
	  • debug-config – Displays smart-rf debug configuration information
	  • sensitivity [client|pattern|rates] – Displays the smart-rf sensitivity table.
	  • client {[<0-8192>|<MAC>]} – Displays smart-rf sensitivity information for a selected Client.
	• <0-8192> – Optional. Client index.
	• <MAC> – Optional. Client MAC address.
	  • pattern [pattern-11a|pattern-11b|pattern-11bg|pattern-2-mbps] – Displays smart-rf common Client patterns.
	• pattern-11a – 11a clients
	• pattern-11b – 11b clients
	• pattern-11bg – 11bg clients
	• pattern-2-mbps – 2-Mbps units
	  • rates <rate-flag> – Displays rates. <rate-flag> is in hexadecimal format.
	• wireless [ap-history|buffer-counters|enhanced-beacon-table|enhanced-probe-table|group|group-stats|legacy-load-balance|client-cache-buckets|client-cache-entry|mvlan radio|radio-cache-entry|radio-hash-buckets|snmp-trap-throttle|vlan-cache-buckets|vlan-cache-entry|waiting] – Displays wireless parameters.
	  • ap-history {<MAC>} – Displays access point history for all MACs. Provide the optional <MAC> parameter to view ap-history for a AP with that MAC address.
	  • buffer-counters – Displays allocations for the different buffers.

- enhanced-beacon-table [config|report] – Displays Enhanced Beacon Table information.
  - config – Displays Enhanced Beacon Table configuration information.
  - report – Displays Enhanced Beacon Table reports.
- enhanced-probe-table [config|report] – Displays Enhanced Probe Table information.
  - config – Displays Enhanced Probe Table configuration information.
  - report – Displays Enhanced Probe Table reports
- group <1-256> – Displays information on a radio group.
  - <1-256> – The radio group index to display information for.
- group-stats – Displays radio group statistics.
- legacy-load-balance – Displays legacy load balance algorithm compatibility mode.
- client-cache-buckets – Displays wireless wireless clients cache buckets.
- client-cache-entry [<1-8192>|<MAC>] – Displays Client Cache information, dumps the whole Client Cache table if no parameters is given.
  - <1-8192> – An index in the Client Cache table.
  - <MAC> – MAC address of client-cache entry to show.
- mvlan <1-256> – Displays multi VLAN debug statistics.
  - <1-256> – A single wlan index.
- radio [<1-4096>|description|mapping] – Displays radio serviceability parameters.
  - <1-4096> – A single radio index.
  - description – Description and location co-ordinates of radios.
  - mapping – Radio-to-CPU Mapping.

- radio-cache-entry {<MAC>} – Displays Radio Cache information. Dumps the whole table if no parameter is given.
  - <MAC> – MAC address of radio-cache entry to show.
- radio-hash-buckets – Displays Wireless Radio Hash Buckets.
- snmp-trap-throttle – Displays statistics and parameters related to SNMP Trap Throttling.
- vlan-cache-buckets – Displays wireless VLAN Cache Buckets.
- vlan-cache-entry [<1-8192>|<MAC>] – Displays Client VLAN Cache information. Dumps whole table if no parameter is given.
  - <1-8192> – An index in the Client VLAN Cache table.
  - <MAC> – MAC address of VLAN cache entry to show.
- waiting <0-99> – Displays waiting table contents.
  - <0-99> – Index in the waiting table.

smart-rf [clear-history|load-from-file|replay|rescue|restore|save-to-file|simulate]	Configures smart-rf parameters.
	• clear-history – Clears assignment history.
	• load-from-file – Loads smart-rf configuration from the file *smart.bin*.
	• replay enable – Enables replay mode for smart-rf
	• rescue [<MAC>|<1-4094>|<index-list>] – Forces radio rescue operation.
	  • <MAC> – MAC address of a single radio.
	  • <1-4094> – Radio index.
	  • <index-list> – List of radio indices.

	• restore [<MAC>|<1-4094>|<index-list>] – Removes radio rescue operation on a given radio.
	  • <MAC> – MAC address of a single radio.
	  • <1-4094> – Radio index.
	  • <index-list> – List of radio indices.
	• save-to-file – Saves smart-rf records to the file *smart.bin*.
	• simulate [coverage-hole|interference] – Simulates radio events for smart-rf.
	  • coverage-hole <1-4096> <experienced-range> [<transmit-rate>|pattern-11a|pattern-11b|pattern-11bgn|
	pattern-2-mbps] – Simulates a coverage-hole radio event on the selected radio index.
	  • <1-4096> – The radio index to simulate on.
	  • <experienced-range> – The experienced range in Mbps.
	  • <transmit-rate> – The provide simulated Client's allowed transmit rates in hexadecimal format.
	  • pattern-11a – 11a units
	  • pattern-11b – 11b units
	  • pattern-11bg – 11bg units
	  • pattern-2-mbps – 2 Mbps units
	  • interference [<MAC>|<1-4094>|<index-list>] – Simulates an interference on a radio.
	  • <MAC> – MAC address of a single radio.
	  • <1-4094> – Radio index.
	  • <index-list> – List of radio indices.

wireless [ap-history|
clear-ap-log|custom-cli|
dot11i|dump-core|
enhanced-beacon-table|
enhanced-probe-table|
free-packet-watermark|
idle-radio-send-multicast|
legacy-load-balance|map-radios|
radio-misc-cfg|
rate-scale|
request-ap-log|
save-ap-log|
snmp-trap-throttle|
sync-radio-entries|
vlan-cache]
	Configures wireless parameters.
	• ap-history [clear|enable] – Configures access point history.
	  • clear – Clears all history of all APs.
	  • enable – Enables tracking of AP history.
	• custom-cli [sh-wi-wireless-client|sh-wi-radio] – Customize the output of some summary cli commands in wireless.
	  • sh-wi-wireless-client [ap-locn|ap-name|channel|dot11-type|ip|last-heard|mac|radio-bss|radio-desc|radio-id|ssid|state|vlan|wlan-desc|wlan-id|username] – Customize the output of the '**show wireless wireless-client**' command.
	• ap-locn – The location of the AP where the wireless-client is associated.
	• ap-name – The name of the AP where the wireless-client is associated.
	• channel – The channel of the radio where the wireless-client is associated.
	• dot11-type – The dot11 radio type of the wireless-client.
	• ip – The IP address of the wireless-client.
	• last-heard – The time when a packet was last received from the wireless-client.
	• mac – MAC address of wireless-client.
	• radio-bss – The BSSID of the radio where the wireless-client is associated.
	  • radio-desc – Description of radio where the wireless-client is associated.
	  • radio-id – The radio index to which the wireless-client is associated.
	  • ssid – The SSID of the wireless-clients wlan.
	  • state – The current state of the wireless-client.

- username – The Radius username of the user connected through this device (shown only if applicable and available).
- vlan – The VLAN-ID assigned to the wireless-client.
- wlan-desc – The WLAN description the wireless-client is using.
- wlan-id – The WLAN index the wireless-client is using.

- sh-wi-radio [adopt-info|ap-locn|ap-mac|ap-name|bss|channel|dot11-type|num-client|power|radio-desc|radio-id|state] – Customize the output of the "**show wireless radio**" command.
  - adopt-info – The adoption information about the radio.
  - ap-locn – The location of the AP to which this radio belongs.
  - ap-mac – The MAC address of AP to which the radio belongs.
  - ap-name – The name of the AP to which this radio belongs.
  - bss – The BSSID of the radio.
  - channel –The configured and current channel of the radio.
  - dot11-type – The dot11 type (11a/11g etc) of the radio.
  - num-client – The number of mobile devices associated with this radio.
  - power – The configured and current transmit power of the radio.
  - pref-id – The adoption preference ID of the radio.
  - radio-desc – The description of radio.
  - radio-id – The radio index in configuration.
  - state – The current operational state of the radio.

- dot11i – modify dot11i service parameters.
- dump-core – Creates a core file of the *ccsrvr* process.
- enhanced-beacon-table [channel-set|enable|erase-report|max-ap|scan-interval|scan-time] – Enhanced beacon table for AP locationing.
  - channel-set [a|an|b|bg|bgn] <1-200> – Adds channels to the different radio types. Channel types are a, an, b, bg, bgn. The channel number must be in the range 1 to 200.
  - enable – Enables the Enhance Beacon Table feature for AP locationing.
  - erase-report – Erases the reports for Enhanced Beacon Table feature.
  - max-ap <0-512> – Sets the maximum number of APs to be recorded in the Enhanced Beacon Table. Set a value in the range 0 -512.
  - scan-interval <10-60> – The time duration between two enhanced beacon table for AP locationing scans in seconds.
  - scan-time <100-1000> – The time duration of an Enhanced Beacon Table scan in milliseconds.
- enhanced-probe-table [enable|erase-report|max-client|preferred|window-time] – Enhanced probe table for Client locationing.
  - enable – Enables the Enhanced Probe Table feature for Client locationing.
  - erase-report – Erases the reports for Enhanced Probe Table feature.
  - max-client <0-512> – Sets the maximum clients in the Enhance Probe Table report.
  - preferred <MAC> – Add the MAC <MAC> to the preferred Client list.
  - window-time <10-60> – Sets the Window Time for probe collection in seconds to a value in the range 10 to 60 seconds.

- free-packet-watermark <0-100>– The free packets threshold in percent. If the percentage of free packets is lower than this number, then additional packets will not be queued in the datapath.
- idle-radio-send-multicast enable – Enables forwarding multicast packets to radios without associated wireless clients.
- legacy-load-balance – Invoke legacy load balance algorithm.
- map-radios <1-127> – Sets radio-to-cpu mapping constant to a value in the range of 1 and 127.
- radio-misc-cfg <hex-bitmask> – Radio specific miscellaneous U16 configuration for all radios.
- rate-scale – Enable wireless rate scaling (default).
- request-ap-log <1-1024> – Request AP Log for the selected AP.
- save-ap-log – Saves debug/error logs sent by the access-point
- snmp-trap-throttle <1-20> – Limits the number of SNMP traps generated per second from the wireless module to a number in the range 1 and 20.
- sync-radio-entries – sync radio configuration at cluster levels.
- vlan-cache enable – Enables VLAN-cache mode.

See also, "service" on page 37.

Usage Guidelines

To stop a service, use the no command. For instance, use **no service wireless idle-radio-send-multicast enable** to stop sending broadcast/multicast frames to idle radios

Example

```
RFController(config-wireless)#service show wireless ap-history
AP MAC             Radio  Timestamp          Event       Reason
=================================================================
00-A0-F8-BF-8A-4B  N/A    20100926-20:23:10  Adoption    N/A
RFController(config-wireless)#

RFController(config-wireless)#service show wireless mvlan 20
Wlan 20: pool_size =1
-----------------------------------------------------
[ 0]: wlan=20, vlan_id=1, limit=0, users=0, log_sent=0
[ 1]: wlan=20, vlan_id=0, limit=0, users=0, log_sent=0
[ 2]: wlan=20, vlan_id=0, limit=0, users=0, log_sent=0
[ 3]: wlan=20, vlan_id=0, limit=0, users=0, log_sent=0
[ 4]: wlan=20, vlan_id=0, limit=0, users=0, log_sent=0
[ 5]: wlan=20, vlan_id=0, limit=0, users=0, log_sent=0
[ 6]: wlan=20, vlan_id=0, limit=0, users=0, log_sent=0
[ 7]: wlan=20, vlan_id=0, limit=0, users=0, log_sent=0
[ 8]: wlan=20, vlan_id=0, limit=0, users=0, log_sent=0
[ 9]: wlan=20, vlan_id=0, limit=0, users=0, log_sent=0
[10]: wlan=20, vlan_id=0, limit=0, users=0, log_sent=0
[11]: wlan=20, vlan_id=0, limit=0, users=0, log_sent=0
[12]: wlan=20, vlan_id=0, limit=0, users=0, log_sent=0
[13]: wlan=20, vlan_id=0, limit=0, users=0, log_sent=0
[14]: wlan=20, vlan_id=0, limit=0, users=0, log_sent=0
[15]: wlan=20, vlan_id=0, limit=0, users=0, log_sent=0
```

```
[16]: wlan=20, vlan_id=0, limit=0, users=0, log_sent=0
[17]: wlan=20, vlan_id=0, limit=0, users=0, log_sent=0
[18]: wlan=20, vlan_id=0, limit=0, users=0, log_sent=0
[19]: wlan=20, vlan_id=0, limit=0, users=0, log_sent=0
[20]: wlan=20, vlan_id=0, limit=0, users=0, log_sent=0
[21]: wlan=20, vlan_id=0, limit=0, users=0, log_sent=0
[22]: wlan=20, vlan_id=0, limit=0, users=0, log_sent=0
[23]: wlan=20, vlan_id=0, limit=0, users=0, log_sent=0
[24]: wlan=20, vlan_id=0, limit=0, users=0, log_sent=0
[25]: wlan=20, vlan_id=0, limit=0, users=0, log_sent=0
[26]: wlan=20, vlan_id=0, limit=0, users=0, log_sent=0
[27]: wlan=20, vlan_id=0, limit=0, users=0, log_sent=0
[28]: wlan=20, vlan_id=0, limit=0, users=0, log_sent=0
[29]: wlan=20, vlan_id=0, limit=0, users=0, log_sent=0
[30]: wlan=20, vlan_id=0, limit=0, users=0, log_sent=0
[31]: wlan=20, vlan_id=0, limit=0, users=0, log_sent=0
RFController(config-wireless)#

RFController(config-wireless)#service show wireless radio description
# access-point MAC      start BSS          radio  description coordinates
1]  00-A0-F8-BF-8A-4B  00-A0-F8-BF-EF-B0  11bg   RADIO1               0 0 0
2]  00-A0-F8-BF-8A-4B  00-A0-F8-BF-ED-BC  11a    RADIO2               0 0 0
RFController(config-wireless)#

RFController(config-wireless)#service show wireless snmp-trap-throttle
throttle : 10 (default = 10)
traps allowed through throttle: 9
traps dropped through throttle: 0
RFController(config-wireless)#
```

show

Wireless configuration commands

Displays current system information running on the controller

For other show commands, see *Chapter 2, Section show* on *page 2-59*.

Supported in the following platforms:

- Mobility RFS4000 Controller
- Mobility RFS6000 Controller
- Mobility RFS7000 Controller

NOTE
The following commands display only for the Mobility RFS6000 Controller and the Mobility RFS4000 Controller
- power
The following commands display only for the Mobility RFS7000 Controller and the Mobility RFS4000 Controller:
- port-channel
- static-channel-group

Syntax

```
show <paramater>
```

Parameters

?	Displays all the parameters for which information can be viewed using the show command

Example

```
RFController(config-wireless)#show ?
  aap-wlan-acl                wlan based acl
  aap-wlan-acl-stats          IP filtering wlan based statistics
  access-list                 Internet Protocol (IP)
  aclstats                    Show ACL Statistics information
  alarm-log                   Display all alarms currently in the system
  autoinstall                 autoinstall configuration
  banner                      Display Message of the Day Login banner
  boot                        Display boot configuration.
  clock                       Display system clock
  commands                    Show command lists
  crypto                      encryption module
  debugging                   Debugging information outputs
  dhcp                        DHCP Server Configuration
  environment                 show environmental information
  file                        Display filesystem information
  firewall                    Wireless firewall
  ftp                         Display FTP Server configuration
  history                     Display the session command history
  interfaces                  Interface status
  ip                          Internet Protocol (IP)
  ldap                        LDAP server
  licenses                    Show any installed licenses
  logging                     Show logging configuration and buffer
```

```
  mac                          Internet Protocol (IP)
  mac-address-table            Display MAC address table
  mac-name                     Displays the configured mac names
  management                   Display L3 Managment Interface name
  mobility                     Display Mobility parameters
  ntp                          Network time protocol
  password-encryption          password encryption
  port                         Physical/Aggreagte port interface
  port-channel                 Portchannel commands
  privilege                    Show current privilege level
  protocol-list                List of protocols
  radius                       RADIUS configuration commands
  redundancy                   Display redundancy group parameters
  role                         Configure role parameters
  rtls                         Real Time Locating System commands
  running-config               Current Operating configuration
  securitymgr                  Securitymgr parameters
  service-list                 List of services
  sessions                     Display current active open connections
  smtp-notification            Display SNMP engine parameters
  snmp                         Display SNMP engine parameters
  snmp-server                  Display SNMP engine parameters
  spanning-tree                Display spanning tree information
  startup-config               Contents of startup configuration
  static-channel-group         static channel group membership
  terminal                     Display terminal configuration parameters
  timezone                     Display timezone
  traffic-shape                Display traffic shaping
  upgrade-status               Display last image upgrade status
  users                         Display information about currently logged in
                               users
  version                      Display software & hardware version
  virtual-ip                   IP redundancy feature
  wireless                     Wireless configuration commands
  wlan-acl                     wlan based acl

RFController(config-wireless)#show

RFController(config-wireless)#show wireless config
country-code             : us
adoption-pref-id         : 1
proxy-arp                : enabled
adopt-unconf-radio       : disabled
dot11-shared-key-auth    : disabled
ap-detection             : disabled
manual-wlan-mapping      : disabled
dhcp sniff state         : disabled
dhcp fix broadcast-rsp   : disabled
broadcast-tx-speed       : optimize-for-range
wlan bw allocation       : enabled
Adaptive ap parameters:
 config-apply def-delay : 30 seconds
 config-apply mesh-delay: 3 minutes
wired-to-wireless rate limit per user : unlimited
wireless-to-wired rate limit per user : unlimited
user load balance mode  : by-throughput
.............................................................
.............................................................
.............................................................
RFController(config-wireless)
```

```
RFController(config-wireless)#show wireless radio-group
 group_id   | radios
 ------------------------------------------------------------
         11 | 1,4
RFController(config-wireless)#

RFController(config-wireless)#show wireless ap
Number of access-ports adopted   : 0
Number of AAPs adopted           : 0
Available AP licenses            : 0
Available AAP licenses           : 0
Redundancy enabled               : N
Redundancy mode                  : active
RFController(config-wireless)#


RFController(config-wireless)show service-list
qmtp                    209/tcp
qmtp                    209/udp
z3950                   210/tcp
z3950                   210/udp
ipx                     213/tcp
ipx                     213/udp
imap3                   220/tcp
imap3                   220/udp
rpc2portmap             369/tcp
rpc2portmap             369/udp
codaauth2               370/tcp
codaauth2               370/udp
ulistserv               372/tcp
ulistserv               372/udp
ldap                    389/tcp
ldap                    389/udp
https                   443/tcp
https                   443/udp
snpp                    444/tcp
snpp                    444/udp
ssmtp                   465/tcp
saft                    487/tcp
saft                    487/udp
exec                    512/tcp
biff                    512/udp
login                   513/tcp
who                     513/udp
hell                    514/tcp
syslog                  514/udp
printer                 515/tcp
talk                    517/udp
ntalk                   518/udp
route                   520/udp
timed                   525/udp
tempo                   526/tcp
courier                 530/tcp
conference              531/tcp
netnews                 532/tcp
netwall                 533/udp
gdomap                  538/tcp
gdomap                  538/udp
uucp                    540/tcp
```

```
klogin                  543/tcp
kshell                  544/tcp
afpovertcp              548/tcp
afpovertcp              548/udp
remotefs                556/tcp
nntps                   563/tcp
nntps                   563/udp
nqs                     607/tcp
npmp-local              610/tcp
npmp-local              610/udp
npmp-gui                611/tcp
npmp-gui                611/udp


RFController(config-wireless)#show wireless radio
IDX AP MAC             RADIO-BSSID       TYPE STATE CHANNEL POWER ADOPTED-BY
1   00-A0-F8-00-00-00 00-23-68-2E-7E-F8 11bgn normal 6  (acs) 8 (8 )
current-controller
2   00-A0-F8-00-00-00 00-23-68-2E-7A-18 11an normal  104(rnd) 18(20)
current-controller
3   00-A0-F8-BF-8A-70 00-A0-F8-BF-F1-44 11bg normal  11 (rnd) 20(20)
current-controller
4   00-A0-F8-BF-8A-70 00-A0-F8-BF-EE-3C 11a normal   149 (rnd) 20(20)
current-controller
5   00-A0-F8-BF-89-45 00-A0-F8-BF-E5-5C 11bg normal  1   (rnd) 20(20)
current-controller
6   00-A0-F8-BF-89-45 00-A0-F8-BF-E6-08 11a normal   36  (rnd) 17(20)
current-controller
RFController(config-wireless)#show wireless radio statistics 2 detail

Rates(Mbps)                                    Tx packets Rx Packets
---------------------------------------- ---------- -------
802.11b rates (1, 2, 5.5, 6)                        0        0
802.11a/g low rates (9, 11, 12)                     0        0
802.11a/g low rates (18, 22, 24)                    0        0
802.11a/g high rates (36, 48, 54)                   0        0
802.11n (MCS 0-3)                                   0        0
802.11n (MCS 4-7)                                   0        0
802.11n (MCS 8-11)                                  0        0
802.11n (MCS 12-15)                                 0        0

Voice:
Rates(Mbps) Tx packets Rx Packets
----------- ---------- ----------
1.0             0           0
2.0             0           0
5.5             0           0
6.0             0           0
9.0             0           0
11.0            0           0
12.0            0           0
18.0            0           0
22.0            0           0
24.0            0           0
36.0            0           0
48.0            0           0
54.0            0           0

Retry Counts Packets
------------ -------
```

```
0                0
1                0
2                0
3                0
4                0
5                0
6                0
7                0
8                0
9                0
10               0
11               0
12               0
13               0
14               0
15               0
Voice failed : 0
Tx BCMC drops : 0

RFController(config-wireless)#show wireless wlan statistics 1 detail

Rates(Mbps)                                  Tx packets Rx Packets
-------------------------------------------- ---------- -------
802.11b rates (1, 2, 5.5, 6)                          0         0
802.11a/g low rates (9, 11, 12)                       0         0
802.11a/g low rates (18, 22, 24)                      0         0
802.11a/g high rates (36, 48, 54)                     0         0
802.11n (MCS 0-3)                                     0         0
802.11n (MCS 4-7)                                     0         0
802.11n (MCS 8-11)                                    0         0
802.11n (MCS 12-15)                                   0         0
Voice:
Rates(Mbps) Tx packets Rx Packets
----------- ---------- ----------
1.0               0          0
2.0               0          0
5.5               0          0
6.0               0          0
9.0               0          0
11.0              0          0
12.0              0          0
18.0              0          0
22.0              0          0
24.0              0          0
36.0              0          0
48.0              0          0
54.0              0          0
Retry Counts Packets
------------ -------
0               0
1               0
2               0
3               0
4               0
5               0
6               0
7               0
8               0
9               0
10              0
```

```
11              0
12              0
13              0
14              0
15              0
Voice failed : 0
RFController#show wireless client
IDX MAC/NAME RADIO TYPE WLAN VLAN READY IP-ADDRESS
LAST ACTIVE
2 00-1E-E5-EA-1D-60 2 11bg 1 1 Y
192.168.1.194 359 Sec
Number of clients associated: 1

RFController#show wireless client statistics 00-1E-E5-EA-1D-60 detail

mu_idx = 1
Voice
Rates(Mbps) Tx packets Rx Packets Tx packets Rx Packets
----------- ---------- ---------- ---------- ----------
1.0               0          8          0          0
2.0               0          0          0          0
5.5               0          0          0          0
6.0               0          0          0          0
9.0               0          0          0          0
11.0              0          0          0          0
12.0              0          0          0          0
18.0              0          0          0          0
22.0              0          0          0          0
24.0              0          0          0          0
36.0              1          0          0          0
48.0              0          0          0          0
54.0              5          0          0          0

Retry Counts Packets
------------ -------
0               4
1               1
2               1
3               0
4               0
5               0
6               0
7               0
8               0
9               0
10              0
11              0
12              0
13              0
14              0
15              0

Voice failed : 0

RFController#
RFController#show wireless client

IDX MAC/NAME            RADIO TYPE WLAN VLAN READY IP-ADDRESS LAST ACTIVE
2   00-1E-E5-EA-1D-60 4   11an      1     1    Y   192.168.1.194 76 Sec
```

```
Number of clients associated: 1



RFController#show wireless client statistics 00-1E-E5-EA-1D-60 detail

mu_idx = 1
Rates(Mbps)                                  Tx packets Rx Packets
-------------------------------------------- ---------- -------
802.11b rates (1, 2, 5.5, 6)                          0       18
802.11a/g low rates (9, 11, 12)                       0        0
802.11a/g low rates (18, 22, 24)                      0        5
802.11a/g high rates (36, 48, 54)                     0        5

Voice:
Rates(Mbps) Tx packets Rx Packets
----------- ---------- ----------
1.0                 0          0
2.0                 0          0
5.5                 0          0
6.0                 0          0
9.0                 0          0
11.0                0          0
12.0                0          0
12.0                0          0
18.0                0          0
22.0                0          0
24.0                0          0
36.0                0          0
48.0                0          0
54.0                0          0
Retry Counts Packets
------------ -------
     0          2
     1          0
     2          0
     3          0
     4          0
     5          0
     6          0
     7          0
     8          0
     9          0
     10         0
     11         0

RFController#show wireless radio
IDX AP MAC            RADIO-BSSID       TYPE STATE CHANNEL POWER ADOPTED-BY
1   00-A0-F8-00-00-00 00-0B-6B-B1-E4-90 11bgn normal 11    (rnd)  4 (4 )
current-controller
4   00-A0-F8-00-00-00 00-0B-6B-B1-E4-88 11an normal 48     (rnd)  4 (4 )
currenkt-controller

RFController#

RFController#show wireless radio statistics 1 detail

Rates(Mbps)                                  Tx packets Rx Packets
-------------------------------------------- ---------- -------
802.11b rates (1, 2, 5.5, 6)                        303       0
```

```
802.11a/g low rates (9, 11, 12)                  0        0
802.11a/g low rates (18, 22, 24)                 0        0
802.11a/g high rates (36, 48, 54)                0        0
802.11n (MCS 0-3)                                0        0
802.11n (MCS 4-7)                                0        0
802.11n (MCS 8-11)                               0        0
802.11n (MCS 12-15)                              0        0

Voice:
Rates(Mbps) Tx packets Rx Packets
----------- ---------- ----------
    1.0          0           0
    2.0          0           0
    5.5          0           0
    6.0          0           0
    9.0          0           0
    11.0         0           0
    12.0         0           0
    18.0         0           0
    22.0         0           0
    24.0         0           0
    36.0         0           0
    48.0         0           0
    54.0         0           0
Retry Counts Packets
------------ -------
      0          303
      1          0
      2          0
      3          0
      4          0
      5          0
      6          0
      7          0
      8          0
      9          0
      10         0
      11         0
      12         0
      13         0
      13         0
      14         0
      15         0
Voice failed : 0
Tx BCMC drops : 0
RFController#
```

smart-rf

Wireless configuration commands

Configures Smart-RF Management parameters and moves to the `(config-wireless-smart-rf)` instance

Supported in the following platforms:

- Mobility RFS4000 Controller
- Mobility RFS6000 Controller
- Mobility RFS7000 Controller

NOTE

`smart-rf` initiates the `(config-wireless-smart-rf)` instance. For more details see *Chapter 25, Smart RF Instance*. The prompt changes from `RFController (config-wireless)#` to `RFController (config-wireless-smart-rf)`

Syntax

```
smart-rf
```

Parameters

None

Example

```
RFController(config-wireless)#smart-rf
RFController(config-wireless-smart-rf)#
```

smart-scan-channels

Wireless configuration commands

Specifies a list of channels for Brocade clients to do smart-scan

Supported in the following platforms:

- Mobility RFS4000 Controller
- Mobility RFS6000 Controller
- Mobility RFS7000 Controller

Syntax

```
smart-scan-channels [<channel-list>|add <channel-list>|
       remove <channel-list>]
```

Parameters

<channel-list>	A comma-separated list of channels
add <channel-list>	Add one or more channels to existing channel list
remove <channel-list>	Remove one or more channels from existing channel list

Example

```
RFController(config-wireless)#smart-scan-channels add 1,3,4
```

wlan

Wireless configuration commands

Configures Wireless LAN related commands

Supported in the following platforms:

- Mobility RFS4000 Controller
- Mobility RFS6000 Controller
- Mobility RFS7000 Controller

NOTE
Manual mapping of wlan will be erased when the actual wlan is disabled and enabled.

Syntax

```
wlan [<1-256>|<wlan-list>] [80211-extensions|802.11w-mfp|

aap-ipfilter-rules|aap-proxy-radius|accounting|acl|add-vlan|answer-bcast-ess|
       authentication-type|client-bridge-backhaul|
     deny-static-mu|description|
dot11i|enable|encryption-type|hold-time|hotspot|
       inactivity-timeout|independent|ip|kdc|mobility|
max-flows-per-mu|
       mu-mu-disallow|nac-mode|nac-server|nas-id|nas-port-id|
       qos|radius|secure-beacon|set-vlan-user-limit|
       smart-scan-channels|ssid|storm-control|syslog|url-log|vlan|wep128|
wep64]
wlan <1-256> [answer-bcast-ess|enable|independent|
       mu-mu-disallow

wlan <1-256> 80211-extensions move-command enable
wlan <1-256> 802.11w-mfp optional required sa-query
wlan <1-256> aap-proxy-radius enable realm <realm name>
       strip
wlan <1-256> accounting [none|radius|ssyslog]
wlan <1-256> acl exceed-rate mu-denied-traffic <0-10000000>
       disassociate
wlan <1-256> add-vlan [<1-4094>|<vlan-list>]
       {limit <0-4096>}
wlan <1-256> authentication-type [eap|hotspot|kerberos|
       mac-auth|none]
wlan <1-256> aap-ipfilter-rules [in|out]
{<1-20>|AAP_IPF_RULE}
wlan <1-256> client-bridge-backhaul enable
wlan <1-256> description <description>

wlan <1-256> dot11i [handshake|key|key-rotation|
       key-rotation-interval|opp-pmk-caching|phrase|pmk-caching|
       preauthentication|second-key|tkip-cntrmeas-hold-time|
       wpa2-tkip]
wlan <1-256> dot11i [opp-pmk-caching|pmk-caching|
       preauthentication
wlan <1-256> dot11i handshake timeout <100-5000>
       retransmit <1-10>
wlan <1-256> dot11i key [0 <secret-key>|2 <secret-key>|
       <secret-key>]
```

```
wlan <1-256> dot11i key-rotation enable
wlan <1-256> dot11i key-rotation-interval <30-86400>
wlan <1-256> dot11i phrase [0 <secret-key>|2 <secret-key>|
       <secret-key>]
wlan <1-256> dot11i second-key [enable|key|phrase]
wlan <1-256> dot11i second-key enable
wlan <1-256> dot11i second-key [key|phrase] [0 <secret-key>|
       2 <secret-key>|<secret-key>]
wlan <1-256> dot11i tkip-cntrmeas-hold-time <0-65535>
wlan <1-256> dot11i wap2-tkip enable

wlan <1-256> encryption-type [ccmp|keyguard|none|tkip|
       tkip-ccmp|wep128|wep128-keyguard|wep64]
wlan <1-256> hold-time <1-300>

wlan <1-256> hotspot
[allow-eap|allow-list|authentication|cache-ageout|connwction-mode|
dns-whitelist|ntf-logout-port|portal-ip|
pre-auth-vlan|query|redirect-to-hostname|
    simultaneous-users|webpage|webpage-location]
wlan <1-256> hotspot [allow-eap|redirect-to-hostname
wlan <1-256> hotspot allow-list <1-32> <IP>
wlan <1-256> hotspot authentication[free|radius]
wlan <1-256> hotspot cache-ageout <5-86400>
wlan <1-256> hotspot connection-mode [http|https]
wlan <1-256> hotspot ntf-logout-port <0-65535>
wlan <1-256> hotspot portal-api [enable|shared-secret <LINE>]
wlan <1-256> hotspot pre-auth-vlan <1-4096>
wlan <1-256> hotspot simultaneous-users <0-8192>
wlan <1-256> hotspot webpage [external|internal]
       [failure|login|welcome] <URL>
wlan <1-256> hotspot webpage-location
       [advanced|external|internal {logout-on-browser-close}]

wlan <1-256> inactivity-timeout <60-86400>

wlan <1-256> ip [arp|dhcp]
wlan <1-256> ip arp [rate-limit <1-1000000>|trust]
wlan <1-256> ip dhcp trust

wlan <1-256> kdc [password|realm|server]
wlan <1-256> kdc password [0 <secret>|2 <secret>|<secret>]
wlan <1-256> kdc realm <realm>
wlan <1-256> kdc server [primary|secondary|timeout]
wlan <1-256> kdc server primary <IP> {auth-port <port>}
wlan <1-256> kdc server secondary <IP> {auth-port <port>}
wlan <1-256> kdc server timeout <1-60>

wlan <1-256> mobility enable

wlan <1-256> nac-mode [bypass-nac-except-include-list|
       do-nac-except-exclude-list|none]
wlan <1-256> nac-server [primary|secondary|timeout]
wlan <1-256> nac-server [primary|secondary]
       [<IP> {auth-port <port>}|radius-key [0 <secret>|
       2 <secret>|<secret>]]
wlan <1-256> nac-server timeout <1-300> retransmit <1-100>

wlan <1-256> nas-id <nas-id>
wlan <1-256> nas-port-id <port>
```

```
wlan <1-256> qos [classification|mcast-with-dot11i|mcast1|
       mcast2|prioritize-voice|rate-limit|svp|weight|wmm]
wlan <1-256> qos classification [low|normal|video|voice|wmm]
wlan <1-256> qos mcast-with-dot11i enable
wlan <1-256> qos [mcast1|mcast2] <MAC>
wlan <1-256> qos prioritize-voice
wlan <1-256> qos rate-limit [wired-to-wireless|
       wireless-to-wired] <100-1000000>
wlan <1-256> qos svp enable
wlan <1-256> qos weight <1-10>
wlan <1-256> qos wmm [8021p|background|best-effort|dscp|
       video|voice]
wlan <1-256> qos wmm [8021p|dscp]
wlan <1-256> qos wmm [background|best-effort|video|voice]
[aifsn <2-15>|cw <0-15> <0-15>|txop-limit <0-65535>]

wlan <1-256> radius [accounting|authentication-protocol|
       dscp|dynamic-authorization|dynamic-vlan-assignment|
       mac-auth-format|client|reauth|server]
wlan <1-256> radius accounting [mode|server|timeout]
wlan <1-256> radius accounting mode [start-interim-stop
       interval <60-3600>|start-stop|stop-only]
wlan <1-256> radius accounting server [primary|secondary] [<IP> {acct-port
<port>}|radius-key [0 <key>|2 <key>|<key>]]
wlan <1-256> radius accounting timeout <1-60> retransmit
       <1-100>
wlan <1-256> radius authentication-protocol [chap|pap]
wlan <1-256> radius dscp <0-63>
wlan <1-256> radius [dynamic-authorization|
       dynamic-vlan-assignment] enable
wlan <1-256> radius mac-auth-format [no-delim|pair-colon|
       pair-dash|quad-dot|middle-dash]
wlan <1-256> radius client timeout <1-10>
       retransmit <1-10>
wlan <1-256> radius reauth <30-65535>
wlan <1-256> radius server [primary|secondary|timeout]
wlan <1-256> radius server [primary|secondary] [<IP>
       {auth-port <1024-65535>}|radius-key [0 <key>|2 <key>|
       <key>]
wlan <1-256> radius server timeout <1-60> retransmit <1-10>

wlan <1-256> secure-beacon
wlan <1-256> set-vlan-user-limit [<1-4094>|<vlan-list>]
       <0-8192>
wlan <1-256> smart-scan-channels [<channel-list>|add <channel-list>|remove
<channel-list>]
wlan <1-256> ssid <ssid>
wlan <1-256> storm-control [bcast|mcast|ucast]
       rate-limit <1-1000000>
wlan <1-256> syslog accounting server <IP> {port <1-65535>}

wlan <1-256> vlan [<1-4094>|<vlan-list>] {limit <0-8192>}

wlan <1-256> [wep64|wep128] [key|phrase|wep-default-key]
wlan <1-256> [wep64|wep128] key <1-4> [ascii|hex]
       [0 <key>|1 <key>|<key>]
wlan <1-256> [wep64|wep128] phrase <pass-phrase>
wlan <1-256> [wep64|wep128] wep-default-key <1-4>
```

Parameters

<1-256>	Defines a single WLAN index
<wlan-list>	Sets a list (1,3,7) or range (3-7) of WLAN indices

For each of the options <1-256> and <wlan-list> the following commands are available.

80211-extensions move-command enable	Enables support for 802.11 extensions. • move-command – Enables support for fast roaming. • enable – Enables this extension.

802.11w-mfp optional required sa-query	Enables 802.11w Management frame protection settings
	• optional – MFP optional
	• required – MFP required
	  • sa-query [max-timeout|retry-timeout] – Enables SA Query protocol settings
	  • max-timeout – Displays maximum timeout
	  • retry-timeout – Displays retry timeout

aap-proxy-radius enable realm <realm-name> strip	Enables configuring of proxying AAP RADIUS requests. • realm <realm-name> – Provide proxy realm name. • strip – Strip realm name while proxying requests.
accounting [none|radius|syslog]	Defines the accounting configuration on this WLAN. • none – No accounting performed on this WLAN. • radius – Uses RADIUS accounting on this WLAN. • syslog – Uses Syslog accounting on this WLAN.
acl exceed-rate client-denied-traffic <0-1000000> disassociate	Sets the actions taken based on the ACL configuration. • exceed-rate – Action is taken when rate exceeds a set value. • client-denied-traffic – The action is to deny traffic to the Client. • <0-1000000> – The rate of packets / second after exceeding which the traffic from the Client is denied access. • disassociate – When enabled, the Client is disassociated.
add-vlan [<1-4094>|<vlan-list>] *{limit <1-4094>}*	Instead of starting a new VLAN assignment for given WLAN, this command adds a VLAN assignment to an existing VLAN assignment. All prior VLAN settings are retained. • [<1-4094>|<vlan-list>] – Sets the VLAN range list <vlan-list>. It can be either a single index or a list (1,3,7) or range (3-7). • limit – Sets user limits on VLANs to a value in the range <1-4094> for this WLAN. **NOTE:** The `[no]` form of `add-vlan` command deletes the specified VLAN mapping over the specified WLAN range list. If the specified mapping does not exist for a particular WLAN, a “specified vlan does not exists” message displays. The delete action continues on remaining VLANs. If all the VLANs are deleted a default VLAN assignment takes effect.
answer-bcast-ess	Allows this WLAN to respond to probes for broadcast ESS.

authentication-type [eap|hotspot|kerberos| mac-auth|none]	Sets the authentication type for this WLAN. • eap – EAP authentication (802.1X). • hotspot – Web based authentication. • kerberos – Kerberos authentication (encryption will change to WEP128 if its not already wep128/keyguard). • mac-auth – MAC authentication (RADIUS lookup of MAC address). • none – No authentication is used.

wlan <1-256> aap-ipfilter-rules [in|out] {<1-20>|AAP_IPF_RULE}	Configures AAP IP Filter rules
	• in - In direction
	• out - Out direction
	  • <1-20> - A single index
	  • <AAP_IPF_RULE> - A list (for example: 1.3.7) or a range (for example 3-7) of indices

client-bridge-backhaul enable	Enables the client bridge backhaul capability on this wlan.
deny-static-client	Drop packets from static clients
description <description>	Sets the description for this WLAN. Use to identify the selected WLAN.

dot11i [handshake | key| key-rotation | key-rotation-interval| opp-pmk-caching | phrase|pmk-caching | preauthentication | second-key| tkip-cntrmeas-hold-time| wpa2-tkip]	Modifies tkip/ccmp (802.11i) related parameters.
	• handshake timeout <100-5000> retransmit <1-10> – Sets a handshake for the timeout and retransmission intervals.
	  • timeout <100-5000> – Sets the timeout (in milliseconds) between retries.
	  • retransmit <1-10> – Sets the number of retransmission attempts.
	• key [0 <secret-key>|2 <secret-key>|<secret-key>] – Configure the key (PMK).
	  • 0 <secret-key>– Password is specified unencrypted.
	  • 2 <secret-key>– Password is encrypted with password-encryption secret.
	  • <secret-key> – The 256bit (64 hex characters) long key.
	• key-rotation enable – Controls the periodic update of broadcast keys for associated wireless clients.
	• key-rotation-interval <30-86400> – Configures the broadcast key rotation interval in seconds.
	• opp-pmk-caching – Enables the opportunistic use of cached pairwise master keys (fast roaming with eap/802.1X).
	• phrase [0 <secret-key>|2 <secret-key>|<secret-key>] – Configures the passphrase.
	  • 0 <secret-key> – Password is specified unencrypted.
	  • 2 <secret-key> – Password is encrypted with password-encryption secret.
	  • <secret-key> – Set a passphrase between 8 and 63 characters.
	• pmk-caching – Enables the use of cached pairwise master keys (fast roaming with eap/802.1X).
	• preauthentication – Enables support for 802.11i pre-authentication.

	• second-key [enable|key|phrase] – Configures a secondary set of key/passphrase for this WLAN.
	  • enable – Enables the use of a secondary key/passphrase.
	  • key [0 <secret-key>|2 <secret-key>|<secret-key>] – Configures the key (PMK).
	  • phrase [0 <secret-key>|2 <secret-key>|<secret-key>] – Configures the passphrase.
	  • 0 <secret-key>– Password is specified as unencrypted.
	  • 2 <secret-key>– Password is encrypted with password-encryption secret.
	  • <secret-key> – Sets the 256bit (64 hex characters) key.
	• tkip-cntrmeas-hold-time <0-65535> – Configures the hold-time (in seconds) that clients are blocked when TKIP counter measures are invoked. Default is 60 seconds.
	• wpa2-tkip enable – Enables support for WPA2-TKIP (in addition to WPA-TKIP) when TKIP is enabled on this WLAN.

enable	Enables specified WLAN(s).
encryption-type [ccmp|keyguard|none|tkip|tkip-ccmp|wep128|wep64|web128-keyguard]	Sets the encryption type for this WLAN. Options include: • ccmp – AES Counter Mode CBC-MAC Protocol (AES-CCM CCMP). • keyguard – Keyguard-MCM (Mobile Computing Mode). • none – No encryption. • tkip – Enables *Temporal Key Integrity Protocol* (TKIP). • tkip-ccmp – Enables both TKIP and CCMP on this WLAN. • wep128 – Enables *Wired Equivalence Privacy* (WEP) with 128 bit keys. • wep128-keyguard – Enables WEP128 as well as Keyguard-MCM on this WLAN. • wep64 – Enables *Wired Equivalence Privacy* (WEP) with 64 bit keys. **NOTE:** A WEP64 configuration is insecure when two WLANs are mapped to the same VLAN, and one uses no encryption and the other uses WEP.
hold-time <1-300>	Specifies the time duration in seconds to hold user credentials when a Client leaves or roams out.

hotspot [allow-eap|allow-list|authentication|dn-whitelist|cache-ageout|connection-mode|ntf-logout-port|portal-api|pre-auth-vlan|redirect-to-hostname|simultaneous-users|query|webpage|webpage-location]	Modifies hotspot related parameters
	• allow-eap – allow EAP authentication in addition to web based login.
	• allow-list <1-32> <IP> – Specifies the allowed list that user can access without prior authentication. Typically this would be the external web-page's IP address.
	  • <1-32> – Allow-list Rule index value.
	  • <IP> – Allow-list IP address. This parameter refers to a specific IP address to which unauthenticated wireless-clients can connect to. It does not specify a network or a subnet.
	• authentication [free|radius] – Sets authentication type for singed users
	  • free – Provides the user a guest login option.
	  • radius – Provides radius authentication option to login
	• dns-whitelist <WORD> – Configures host whitelist.
	  • LINE – Whitelist name.
	• cache-ageout <5-86400> – The time duration in seconds to ageout the cache after Client disassociation.
	• connection-mode [https|https] – Configures the connection mode as http or https
	  • http – Specifies connection-mode as http
	  • https – Specifies connection-mode as https
	• ntf-logout-port <0-65535> – Configures the port to send the NTF-Logout when the device is in external hotspot mode.
	• Portal-api [enable|shared-secret <LINE>] – Configures the HTTPS-POST API interface used by external web portals
	  • enable – Enables support for the HTTPS-POST API.
	  • shared-secret <LINE> – Configures the security shared-secret between the web portal and the switch
	• pre-auth-vlan <1-4096> – Configures default vlan to be used until users get authorized. Specify the index of the vlan
	• max-login-attempts <0-10> – Modifies hotspot maximum login attempts.
	  • <0-10> – Login attempts between 0-10.
	• query [<1-10>|<query-list>] – Specifies queries to be appended to redirection URL.
	  • <1-10> – A single index.
	  • <query-list> – A list of indices.
	• redirect-to-hostname – Use the Hostname/System-Name in the redirection URL instead of the IP address of the controller.
	• simultaneous-users <0-8192> – Specifies how many simultaneous MAC address can be allowed for a given end user.
	  • <0-8192> – The number of MAC addresses that are allowed to use that username at the same time. 0 implies disabling of the checks.

- webpage external [failure|login|welcome] <URL> – Modifies hotspot page parameters.
  - external – Modifies a hotspot's External Web page.
  - failure – When login fails.
  - login – When login succeeds.
  - welcome – The page to display to welcome user.
  - <URL> – Sets the path to the file to be displayed.

NOTE: When using authentication server, the URL parameters ip_address and port are required when the external entity that serves the pages and authentication server are not the same.

```
http://<external_url>
<login|welcome|fail>.html?ip_address=<a.b.c
.d>&port=<x>

where:
```

- <url> is the url of the server serving the web pages
- <login|welcome|fail>.html is the name of the file to be served
- ip_address=<a.b.c.d> is the IP address of the authentication server. The default ip_address is the same as the IP of the server that is serving the pages
- port=<x> is the port on the authentication server. The default port is 444.
  - internal – Modifies hotspot's Internal Web pages. The following page parts can be defined and modified. You can enter upto 1024 characters for each parameter.
    - description – The description of the page.
    - footer – The footer for the page.
    - header - The page header.
    - main-logo – The main logo for the page.
    - small-logo – A small logo for the page.
    - title – The page title.

	NOTE: The full syntax for the internal page definition is as follows: • `wlan 1 hotspot webpage internal welcome title Welcome to hotspot page. You have logged on successfully`failure – Users are redirected to this Web page if they fail authentication. File must be named *fail.html*. • login – Users are prompted for their username and password within this Web page. File must be named *login.html*. • welcome – Users are redirected to this Web page after they authenticate successfully. File must be named *welcome.html*. • webpage-location [advanced|external|internal] – The location of the Web pages used for authentication. These pages can either be hosted on the controller or an external Web Server. • advanced – Invokes login/welcome/failure Web pages created by the user on the controller. • external – Invokes login/welcome/failure Web pages on an external server. • internal (logout-on-browser-close)– Invokes login/welcome/failure Web pages created automatically on the controller. • logout-on-browser-close – Enables/disables user logout on browser close. Default value `disable`.
ip [arp|dhcp]	Sets Internet Protocol settings for ARP and DHCP packets. • arp [rate-limit <1-1000000>|trust] – Address Resolution Protocol configuration. • dhcp trust – Dynamic Host Resolution Protocol configuration. • trust – Sets the arp/dhcp responses as trusted for this wlan/range. • rate-limit <1-1000000> – Does packet rate limiting on ARP packets to a value in the range 1 and 1000000.
inactivity-timeout <60-86400>	Sets an inactivity timeout in seconds. If a frame is not received from a wireless client for this amount of time, the wireless client is disassociated.
independent	Sets this WLAN to be an independent WLAN.

kdc [password|realm|server]	Modifies KDC related parameters.
	• password [0 <secret>|2 <secret>|<secret>] – Create a KDC server password (up to 127 characters)
	  • 0 <secret>– Password is specified unencrypted.
	  • 2 <secret>– Password is encrypted with a password-encryption secret.
	  • <secret> – Defines a KDC server password (up to 127 characters).
	• realm <realm> – Defines a KDC realm (up to 127 characters).
	  • <realm> – Defines KDC realm (up to 127 characters)
	• server [primary|secondary|timeout] – Modifies KDC server parameters.
	  • primary <IP> {auth-port <port>} – Defines the primary KDC server.
	  • secondary <IP> {auth-port <port>}– Defines the secondary KDC server.
	  • <IP> – Sets the KDC server IP address
	  • auth-port <port> – Optional. Sets the KDC server authentication port to a value in the range 1 to 65535. Default is 88.
	  • timeout <1-60> – Modifies KDC server parameters.
	  • <1-60> – Defines the time the controller waits for a response from the KDC Server before retrying.

mobility enable	Enables L3 Mobility on WLAN(s).
client-client-disallow	Disallows frames from one wireless client to another wireless client on this WLAN.
nac-mode [bypass-nac-except-include-list| do-nac-except-exclude-list|none]	Sets the *Network Access Control (*NAC) mode configuration • bypass-nac-except-include-list – No Client NAC check is done except for those in include list. Devices in the include list have NAC checks. • do-nac-except-exclude-list – A Client NAC check is done except for those in the exclude list. Devices in the exclude list will not have any NAC checks. • none – NAC disabled, no NAC is done. An Client can only get authenticated by a Radius server.

nac-server [primary|secondary| timeout]	Configure a NAC server IP address and an optional authentication port number.
	• [primary|secondary] [<IP> {auth-port <port>}|radius-key [0 <secret>|2 <secret>|<secret>]] – Primary server or secondary server's IP address
	  • <IP> {auth-port <port>} – Set an EAP server IP address and optional EAP server authentication port (default: is 1812)
	  • radius-key [0 <secret>|2 <secret>|<secret>] – Create a Radius server shared secret, up to 127 characters
	  • 0 <secret> – Password is specified as unencrypted
	  • 2 <secret> – Password is encrypted with password-encryption secret
	  • <secret> – Configures a NAC server shared secret
	• timeout <1-300> retransmit <1-100> – Sets the time the controller waits for a response from the RADIUS server before retrying. This is a global setting for both the primary and secondary servers.
	  • retransmit <1-100> – Number of retries before the wireless controller will give up and disassociate wireless client
	  • <1-100> – Retry count
	NOTE: The RFController(config-wireless)# nac-server timeout<*> retransmit<*> should be less than what is defined for an Client's timeout and retries. If the Client's time is less than the server's, a fallback to the secondary server will not work.

nas-id <nas-id>	The nas-id of this wlan to be sent to the RADIUS server. Maximum length of 256 characters.
nas-port-id <port>	The nas-port-od of this wlan to be sent to the RADIUS server. Maximum length of 256 characters.

qos [classification | mcast-with-dot11i| mcast1|mcast2| prioritize-voice| rate-limit|svp|weight| wmm]	Quality of Service commands.
	• classification [background|best-effort|video|voice|wmm] – Select how traffic on this WLAN is classified (relative prioritization on the access point).
	  • low – All traffic on this wlan is treated as low priority traffic (Background).
	  • normal – All traffic on this wlan is treated with normal priority (Best Effort).
	  • video – All traffic on this wlan is treated as Video.
	  • voice – All traffic on this wlan is treated as Voice.
	  • wmm – Use WMM based classification, using DSCP or 802.1p tags to classify traffic into different queues.
	• mcast-with-dot11i enable – Enables multicast mask with dot11i.
	• [mcast1|mcast2] <MAC> – Sets multicast masks.
	  • mcast1 <MAC> – Sets multicast mask for egress prioritization.
	  • mcast2 <MAC> – Sets multicast mask for egress prioritization.
	  • <MAC> – MAC address.
	• prioritize-voice – Prioritize voice frames over general data frames (applies to non-WMM wireless-client).

- rate-limit [wired-to-wireless|wireless-to-wired] <100-1000000> – Sets traffic rate limit for users on the selected WLAN.
  - wired-to-wireless – Down link direction - from network to wireless client.
  - wireless-to-wired – Up link direction - from wireless client to network.
  - <100-1000000> – The rate to limit to in kbps.
- svp enable – Enables support for Spectralink Voice Prioritization.
- weight <1-10> – The egress weight (relative priority to other WLANs) of this WLAN. The weight sets the priority for the packets to be sent.
- wmm [8021p|background|best-effort|dscp|video|voice] – Sets the 802.11e / Wireless Multi Media (WMM) parameters (supported on IP350).
  - 8021p – Use 802.1p frame priority (field in the VLAN tag) to determine packet priority.
  - dscp –Use *Differentiated Services Code Point* (DSCP) bits in the IP header to determine packet priority
  - background [aisfn <2-15>|cw <0-15> <0-15>|txop-limit <0-65535>] – Sets the parameters for background traffic.
  - best-effort [aisfn <2-15>|cw <0-15> <0-15>|txop-limit <0-65535>] – Sets the parameters for normal traffic.
  - video [aisfn <2-15>|cw <0-15> <0-15>|txop-limit <0-65535>] – Sets the parameters for video traffic.
  - voice [aisfn <2-15>|cw <0-15> <0-15>|txop-limit <0-65535>] – Sets the parameters for voice traffic.

    - aisfn <2-15> – *Arbitration Inter Frame Spacing Number* (AIFSN) is the wait time in milliSeconds between data frames. This value is derived using AIFSN and the slot-time.
- <2-15> – The AIFSN spacing number.
    - cw <0-15> <0-15> – *Contention Window* (CW) parameters. Wireless stations pick a number between 0 and the minimum contention window to wait before retrying transmission. Stations then double their wait time on a collision, until it reaches the maximum contention window value.
- <0-15> – CW minimum value. The actual value used is (2^ECWmin - 1)
- <0-15> – CW maximum value. (2^ECWmax - 1).
    - txop-limit <0-65535> – The transmit-opportunity is an interval of time when a particular WMM STA has the right to initiate transmissions onto the wireless medium.
- <0-65535> – The transmit-opportunity in 32 microSecond units.

radius [accounting|
authentication-protocol|
dscp|
dynamic-authorization|
dynamic-vlan-assignment|
mac-auth-format|
wireless-client|
reauth|server]
	Configures RADIUS parameters for the select WLAN.
	• accounting [mode|server|timeout] – Sets RADIUS accounting parameters.
	  • mode [start-stop|stop-only|start-interim-stop] – Sets the Accounting Mode.
	  • start-stop – Sends accounting start-stop.
	  • stop-only – Sends accounting stop-only.
	  • start-interim-stop interval <60-3600> – Sets the time interval between successive accounting updates to a value in the range 60 to 3600 secs.
	  • server [primary|secondary] [<IP> *{acct-port <port>}*|radius-key [0 <key>|2 <key>|<key>]] – Sets the primary or secondary RADIUS server for the selected WLAN.
	  • primary – Sets primary RADIUS server information.
	  • secondary – Sets secondary RADIUS server information.
	  • <IP> – Sets the IP address of the RADIUS server.
	  • acct-port <port> – Sets the optional radius server accounting port. Default is 1813.
	  • radius-key [0 <key>|2 <key>|<key>] – Sets the radius-key for the RADIUS server.
	• 0 <key> – The key is sent unencrypted.
	• 2 <key> – The key is sent encrypted with the password-encryption secret.
	• <key> – The shared key.
	  • timeout <1-300> – Sets the time the wireless controller waits for a response from the RADIUS server before retrying accounting.
	  • <1-300> – The time duration in seconds.

- authentication-protocol [chap|pap] – Sets the RADIUS Authentication Protocol for RADIUS request. Select from CHAP or PAP.
- dscp <0-63> – Specify a *Differentiated Services Code Point* (DSCP) value to provide QoS to RADIUS packets. Set a value in the range 0 to 63.
- dynamic-authorization enable – Configures support for RADIUS dynamic authorization extensions such as Disconnect Message, and Change-Of-Authorization, as described in RFC 3576.
  - enable – Enables this feature.
- dynamic-vlan-assignment enable – Allow users to be assigned to RADIUS server specified VLANs, instead of only the vlan that is mapped to this wlan.
  - enable – Enables this feature.
- mac-auth-format [no-delim|pair-colon|pair-dash|quad-dot|middle-dash] – Set the MAC address format to use.
  - middle-dash – Dash Delimiter in the middle - AABBCC-DDEEFF
  - no-delim – No Delimiter - AABBCCDDEEFF
  - pair-colon – Colon Delimiter per Pair - AA:BB:CC:DD:EE:FF
  - pair-dash – Dash Delimiter per Pair - AA-BB-CC-DD-EE-FF
  - quad-dot – Dot Delimiter per Four Hex - AABB.CCDD.EEFF
- wireless-client timeout <1-300> retransmit <1-100> – Modifies RADIUS/802.1X supplicant related parameters.
  - timeout <1-300> – Sets the Time the wireless controller waits for a response from the wireless-client before retrying. Set a value in the range 1 to 300.
  - retransmit <1-100> – Sets the number of retries before the wireless controller will give up and disassociate the wireless-client. Set a value in the range 1 to 100.

	• server [primary|secondary] [<IP> *{acct-port <port>}*| radius-key [0 <key>|2 <key>|<key>]] – Sets the primary or secondary RADIUS server for the selected WLAN.
	  • primary – Sets primary RADIUS server information
	  • secondary – Sets secondary RADIUS server information.
	  • <IP> – Sets the IP address of the RADIUS server.
	  • acct-port <port> – Sets the optional radius server accounting port. Default is 1813.
	  • radius-key [0 <key>|2 <key>|<key>] – Sets the radius-key for the RADIUS server.
	  • 0 <key> – The key is sent unencrypted.
	  • 2 <key> – The key is sent encrypted with the password-encryption secret.
	  • <key> – The shared key.
	  • timeout <1-300> retransmit <1-100> – Sets the time the controller waits for a response from the RADIUS server before retrying. This is a global setting for both the primary and secondary servers.
	  • retransmit <1-100> – Number of retries before the wireless controller will give up and disassociate wireless client
	• <1-100> – Retry count
	• reauth <30-65535> – Enable periodic reauthentication of all associated wireless-clients.
	  • <30-65535> – The reauthentication interval in seconds.

secure-beacon	Does not include the SSID of this WLAN in beacon frames
set-vlan-user-limit [<1-4094>|<vlan-list>] <0-8192>	Sets user limits on VLANs for this WLAN • [<1-4094>|VLAN] – VLAN range list. It can be either a single index, a list (1,3,7) or a range (3-7) of indices • [<0-8192>] – Sets the VLAN index. The limit is <0-8192>
smart-scan-channels [<channel-list>| add <channel-list>| remove <channel-list>]	Specifies a list of channels to brocade clients to perform a smart-scan. The following are the options set: • <channel-list> – A comma separated list of channels to scan. Can also contain a single channel number. • add <channel-list> – Adds the specified channel(s) to the smart-scan list. • remove <channel-list> – Removes the specified channel(s) from the smart-scan list.
ssid <ssid>	Enter the SSID of this WLAN. <ssid> can be up to 32 characters.
storm-control [bcast|mcast|ucast] rate-limit <rate>	Enables packet dropping in case of flooding attack. • bcast – broadcast packets • mcast – multicast packets • ucast – unicast packets • rate-limit <rate>– Enables rate limiting if the rate exceeds the value set by <rate> (1-1000000 packets/second).
syslog accounting server <IP> *{port <1-65535>}*	Syslog Accounting • accounting – Modifies accounting parameters • server <IP> – Modifies the Syslog accounting server IP Address. • port <1-65535> – Optional. Defines the Syslog server port. The default port number is 514 .

vlan [<1-4094>|<vlan-list>] *{limit <0-8192>}*	Sets the VLAN assignment of this WLAN. This command starts a new VLAN assignment for a WLAN index. All prior VLAN settings are erased. • [<1-4094>|<vlan-list>] –Establishes the VLAN range list. It can be either a single index, a list (1,3,7) or a range (3-7). • limit <0 -8192> – Sets user limits on VLANs for this WLAN.

wep128 [key|phrase|wep-default-key]	Configures WEP128 parameters.
	• key *<1-4>* [ascii|hex] – Configures pre-shared hex keys.
	  • ascii [0 <key>|1 <key>|<key>] – Sets keys as ascii characters (5 characters for wep64, 13 for wep128).
	  • hex [0 <key>|1 <key>|<key>] – Sets keys as hexadecimal characters (10 characters for wep64, 26 for wep128).
	  • 0 <key> – Password is specified unencrypted.
	  • 2 <key> – Password is encrypted with password-encryption secret.
	  • <key> – Key (10 hex or 5 ascii characters for wep64, 26 hex or 13 ascii characters for wep128).
	• phrase <phrase> – Specifies a passphrase from which keys are to be derived.
	  • <phrase> – Sets the passphrase (between 4 and 32 characters).
	• wep-default-key <1-4> – Defines the key index used for transmission from AP to Client.

wep64 [key|phrase|wep-default-key]	Configures WEP64 parameters.
	• key *<1-4>* [ascii|hex] – Configures pre-shared hex keys.
	  • ascii [0 <key>|1 <key>|<key>] – Sets keys as ascii characters (5 characters for wep64, 13 for wep128).
	  • hex [0 <key>|1 <key>|<key>] – Sets keys as hexadecimal characters (10 characters for wep64, 26 for wep128).
	  • 0 <key> – Password is specified unencrypted.
	  • 2 <key> – Password is encrypted with password-encryption secret.
	  • <key> – Key (10 hex or 5 ascii characters for wep64, 26 hex or 13 ascii characters for wep128).
	• phrase <phrase> – Specifies a passphrase from which keys are to be derived.
	  • <phrase> – Sets the passphrase (between 4 and 32 characters).
	• wep-default-key <1-4> – Defines the key index used for transmission from AP to Client.

Example

```
RFController(config-wireless)#wlan 25 accounting syslog
RFController(config-wireless)#

RFController(config-wireless)#wlan 25 answer-bcast-ess
RFController(config-wireless)#

RFController(config-wireless)#wlan 25 authentication-type kerberos
RFController(config-wireless)#

RFController(config-wireless)#wlan 25 description "TestWLAN"
```

```
RFController(config-wireless)#

RFController(config-wireless)#wlan 25 dot11i handshake timeout 2500 retransmit
5
RFController(config-wireless)#

RFController(config-wireless)#wlan 25 dot11i key-rotation enable
RFController(config-wireless)#

RFController(config-wireless)#wlan 25 dot11i key-rotation-interval 2000
RFController(config-wireless)#

RFController(config-wireless)#wlan 25 enable
RFController(config-wireless)#

RFController(config-wireless)#wlan 25 hotspot webpage external failure "This
feature is under development"
RFController(config-wireless)#

RFController(config-wireless)#wlan 25 kdc server primary 1.2.3.4 auth-port
50000
RFController(config-wireless)#

RFController(config-wireless)#wlan 25 mobility enable

RFController(config-wireless)#wlan 1 nac-mode bypass-nac-except-include-list
RFController(config-wireless)#

RFController(config-wireless)#wlan 1 nac-server primary 11.22.33.22 auth-port
1221
RFController(config-wireless)#

RFController(config-wireless)#

RFController(config-wireless)#wlan 25 radius accounting timeout 30 retransmit
50
RFController(config-wireless)#

RFController(config-wireless)#wlan 25 radius wireless-client timeout 30
retransmit 5
RFController(config-wireless)#

RFController(config-wireless)#wlan 25 ssid TestString
RFController(config-wireless)#

RFController(config-wireless)#wlan 25 brocade-extensions fast-roaming enable
RFController(config-wireless)#

RFController(config-wireless)#wlan 25 syslog accounting server 12.13.14.125
port 5005
RFController(config-wireless)#

RFController(config-wireless)#wlan 24 qos mcast-with-dot11i enable
RFController(config-wireless)#wlan 24 storm-control bcast rate-limit 20000

RFController(config-wireless)#wlan 9 aap-ipfilter-rules in 7
RFController(config-wireless)#
```

wlan-bw-allocation

Wireless configuration commands

Enables WLAN bandwidth allocation on all radios

Supported in the following platforms:

- Mobility RFS4000 Controller
- Mobility RFS6000 Controller
- Mobility RFS7000 Controller

Syntax

```
wlan-bw-allocation enable
```

Parameters

enable	Enables WLAN bandwidth allocation on all radios.

Example

```
RFController(config-wireless)#wlan-bw-allocation enable
RFController(config-wireless)#
```

dot11k

Wireless configuration commands

Displays dot11k related commands

Supported in the following platforms:

- Mobility RFS4000 Controller
- Mobility RFS6000 Controller
- Mobility RFS7000 Controller

Syntax

```
dot11k send-beacon-req [<1-8192>|CLIENT|client]
dot11k send-beacon-req <1-8192> measurement-duration <100-10000>
dot11k send-beacon-req [client|CLIENT] <MAC> measurement-duration <100-10000>
```

Parameters

dot11k send-beacon-req [<1-8192>|CLIENT|client]	Triggers the Beacon request send
	• <1-8192> – A single client index
	• CLIENT – A list (eg: 1,3,7) or range (eg: 3-7) of client indices
	• client – client'ss MAC address
	  • MAC – Mac address in AA-BB-CC-DD-EE-FF format
	  • measurement-duration <100-10000> – Specifies measurement duration in TUs
	  • <100-10000> – Specifies range of measurement duration

Example

```
RFController(config-wireless)#dot11k send-beacon-req 9 measurement-duration
777
RFController(config-wireless)#
```

wips

Wireless configuration commands

Configures wips parameters

Supported in the following platforms:

- Mobility RFS7000 Controller

NOTE
This command is not supported on the Mobility RFS6000 Controller and Mobility RFS4000 Controller platform.

Syntax

```
RFController (config-wireless) wips [detect-window
<5-300>|disable|event|reset-to-default]

RFController (config-wireless) wips event
[80211-replay-check-failure|
ad-hoc-advertising-authorized-ssid|ad-hoc-network-violation-authorized-device
|ad-hoc-network-violation-unauthorized-device|
aggressive-scanning |all|ap-default-configuration|
ap-ssid-broadcast-in-beacon|
crackable-wep-iv-key-used|decryption-failures|
dos-association-or-authentication-flood |
dos-broadcast-deauthentication|dos-eapol-start-storm|
dos-unicast-deauthentication-or-disassociation|eap-flood|
eap-nak-flood|failures-reported-by-authentication-servers| fake-ap-flood
frames-from-unassociated-stations
frames-with-bad-essids|fuzzing-all-zero-mac-address-observed
|fuzzing-invalid-frame-type-detected|
fuzzing-invalid-management-frame|
fuzzing-invalid-sequence-number|
identical-source-and-destination-addresses|
impersonation-attack-detected|invalid-8021x-frames|
non-changing-wep-iv|replay-injection-attack|
suspicious-ap-high-rssi|
tkip-mic-counter-measures-caused-by-station|
transmitting-device-using-invalid-mac|
unauthorized-ap-using-authorized-ssid|
unencrypted-station-transmission-detected]{enable|
filter-out <1-86400>|threshold <1-65535>} {authorized|ignored|unauthorized}
```

Syntax

detect-window <duration>	Configures the number of seconds for which information is collected before analysis.Value in the range <5-300>
disable	Disables WIPS without affecting configuration
wips events 80211-replay-check-failure| ad-hoc-advertising-authorized-ssid | ad-hoc-network-violation-authorized-device |ad-hoc-network-violation-unauthorized-device |aggressive-scanning |all| ap-default-configuration | ap-ssid-broadcast-in-beacon| crackable-wep-iv-key-used | decryption-failures | dos-association-or-authentication-flood | dos-broadcast-deauthentication | dos-eapol-start-storm | dos-unicast-deauthentication-or-disassociation |eap-flood | eap-nak-flood | failures-reported-by-authentication-servers | fake-ap-flood |frames-from-unassociated-stations | frames-with-bad-essids |fuzzing-all-zero-mac-address-observed |fuzzing-invalid-frame-type-detected | fuzzing-invalid-management-frame|fuzzing-invalid-sequence-number]	Configures parameters related to the detection of anomalous frames on the RF network. The parameters are: • 80211-replay-check-failure – Detects 802.11 replay failure • ad-hoc-advertising-authorized-ssid – Detects ad-hoc advertising authorized ssid • ad-hoc-network-violation-authorized-device – Enables ad-hoc network violation authorized device • ad-hoc-network-violation-unauthorized-device – Enables ad-hoc network violation unauthorized device • aggressive-scanning – Detects aggressive scanning • all – Enables all types of events • ap-default-configuration – Detects ap default configuration • ap-ssid-broadcast-in-beacon – Detects ap ssid broadcast in beacon • crackable-wep-iv-key-used – Uses crackable wep iv key • decryption-failures – Detects decryption failures • dos-association-or-authentication-flood – Detects dos association or authentication flood • dos-broadcast-deauthentication – Detects dos broadcast - deauthentication • dos-eapol-start-storm – Detects dos eapol-start storm • dos-unicast-deauthentication-or-disassociation – Detects dos unicast deauthentication or disassociation • eap-flood – Detects eap flood • eap-nak-flood – Detects eap-nak-flood • failures-reported-by-authentication-servers – Detects failures reported by authentication servers

wips events [identical-source-and-destination-addresses | impersonation-attack-detected|non-changing-wep-iv|replay-injection-attack | suspicious-ap-high-rssi|tkip-mic-counter-measures-caused-by-station |transmitting-device-using-invalid-mac |unauthorized-ap-using-authorized-ssid|unencrypted-station-transmission-detected] {enable|filter-out|threshold} {authorized|ignored|unauthorized}	• fake-ap-flood– Detects suspected ap flood (based on number of APs observed in a minute) • frames-from-unassociated-stations – Detects frames from unassociated stations • frames-with-bad-essids – filter-ageout <1-86400> – Detects filters age-out duration for the mobile unit frames with bad essids • fuzzing-all-zero-mac-address-observed– Fuzzing: All zero MAC address Observed • fuzzing-invalid-frame-type-detected– Fuzzing: Invalid Frame Type Detected • fuzzing-invalid-management-frame – Fuzzing: Invalid Management Frame • fuzzing-invalid-sequence-number – Fuzzing: Invalid Sequence Number • identical-source-and-destination-addresses – Detects identical source and destination addresses • impersonation-attack-detected – Detects impersonation attack • invalid-8021x-frames – Detects invalid 802.1X frames • non-changing-wep-iv – Detects non-changing wepiv • replay-injection-attack – Detects replay injection attack • suspicious-ap-high-rssi – Detects suspicious ap -high rssi • tkip-mic-counter-measures-caused-by-station – Filters mobile units causing tkip mic counter measures • transmitting-device-using-invalid-mac – Detects transmitting device using invalid MAC • unauthorized-ap-using-authorized-ssid – Detects unauthorized ap using authorized ssid • unencrypted-station-transmission-detected – Detects unencrypted wired leakage

	For the above parameters, the following values are set.
	• enable – Enables monitoring, filtering and triggering alarms
	• filter-ageout <ageout> – Sets the number of seconds mobile units are filtered in the range <1-86400>
	• threshold<1-65535> – Configures the threshold of events allowed in the detection window
	  • authorized – Triggers against authorized devices
	  • ignored – Triggers against ignored devices
	  • unauthorized – Triggers against unauthorized devices

reset-to-default	Reset to default settings

Example

```
RFController(config-wireless)#wips event 80211-replay-check-failure enable
authorized
RFController(config-wireless)#

RFController(config-wireless)#wips event fake-ap-flood threshold 88
RFController(config-wireless)#

RFController(config-wireless)#wips event ad-hoc-advertising-authorized-ssid
filter-ageout 9
RFController(config-wireless)#
```

non-preferred-ap-attempts-threshold

Wireless configuration commands

Displays the number of attempts after which controller will adopt non preferred APs

Supported in the following platforms:

- Mobility RFS4000 Controller
- Mobility RFS6000 Controller
- Mobility RFS7000 Controller

Syntax

```
non-preferred-ap-attempts-threshold <0-20>
```

Parameters

non-preferred-ap-attempts-threshold <0-20>	Displays the number of attempts after which controller will adopt non preferred APs • <0-20> – The number of attempts with numeric value in the range of <0-20> for this wireless-controller

Example

```
RFController(config-wireless)#non-preferred-ap-attempts-threshold 9
RFController(config-wireless)#
```

test

Wireless configuration commands

Testing neighbor report on air

Supported in the following platforms:

- Mobility RFS4000 Controller
- Mobility RFS6000 Controller
- Mobility RFS7000 Controller

Syntax

```
RFSController(config-wireless)test dot11k [make-bcn-rep|
send-beacon-req|send-nbr-rep]
RFSController(config-wireless) test dot11k make-bcn-rep mu <MAC> neighbor
<MAC>

RFSController(config-wireless) test dot11k send-beacon-req
<1-8192> measurement-duration <100-10000>

RFSController(config-wireless) test dot11k send-beacon-req
[mu|MU] <MAC> measurement-duration <100-10000>

RFSController(config-wireless) test dot11k send-nbr-rep mu <MAC> neighbor
```

Parameters

make-bcn-rep mu <MAC> neighbor <MAC>	Making the beacon report • mu – Displays client's mac address • neighbor – Displays neighbor radio's BSS ID • MAC – Displays mac address in AA-BB-CC-DD-EE-FF format

send-beacon-req [<1-8192>|MU|mu]	Triggers the beacon send request
	• <1-8192> – A single index
	• MU – A list (eg: 1,3,7) or range (eg: 3-7) of indices
	• mu – Displays client's mac address
	  • MAC –Displays mac address in AA-BB-CC-DD-EE-FF format
	  • measurement-duration <100-10000> – Specifies measurement duration in TUs
	  • <100-10000> – Specifies range of measurement duration

send-nbr-rep mu <MAC>	Triggers the neighbor report send operation • mu – Displays client's mac address • MAC – Displays mac address in AA-BB-CC-DD-EE-FF format

Example

```
RFController(config-wireless)#test dot11k send-beacon-req 9
measurement-duration 999
RFController(config-wireless)#
```

Chapter

RTLS Instance

21

In this chapter

Use the `(config-rtls)` instance to configure *Real Time Location System* (RTLS) parameters.

To navigate to this instance, use the command

```
RFController(config)#rtls
RFController(config-rtls)#
```

RTLS config commands

This summarizes **`config-rtls`** commands:

TABLE 23 RTLS Commands

Command	*Description*	*Ref.*
aeroscout	Configures aeroscout parameters	*page 706*
clear	Clears locationing information	*page 707*
clrscr	Clears display window	*page 708*
end	Ends the current mode and moves to EXEC mode	*page 709*
espi	Configures ESPI parameters	*page 710*
exit	Ends current mode and moves to the previous mode	*page 711*
help	Description of the interactive help system	*page 712*
ekahau	Configures ekahau parameters	*page 713*
no	Negates a command or sets its defaults	*page 714*
reference-tag	Configures reference tags	*page 716*
rfid	Configures RFID readers	*page 717*
service	Invokes service commands to troubleshoot or debug `(config-rtls)` instance configurations	*page 718*
show	Displays the running system information	*page 721*
site	Configures site parameters	*page 723*
sole	Configures *Smart Opportunistic Location Engine* (SOLE) parameters	*page 724*
controller	Configures controller parameters	*page 725*
zone	Configures zone	*page 726*
ap	Configures AP specific RTLS parameters	*page 727*

aeroscout

RTLS config commands

Configure support for Aeroscout RTLS engine.

Supported in the following platforms:

- Mobility RFS4000 Controller
- Mobility RFS6000 Controller
- Mobility RFS7000 Controller

Syntax

```
aeroscout [enable|multicast-listen-addr<MAC-Address>]
```

Parameters

enable	Enables and configures external Aeroscout RTLS engine
multicast-listen-addr <MAC-Address>	Configures multicast MAC address to which Aeroscout tags packets are destined • <MAC-Address> – Multicast MAC address. AeroScout's default multicast MAC address is '01:0C:CC:00:00:00'.

Usage Guidelines

Use `[no] aeroscout (enable)` to disable support for Aeroscout RTLS engine. This does not affect on-board locationing.

Example

```
RFController(config-rtls)#aeroscout enable
RFController(config-rtls)#
```

clear

RTLS config commands

Clears tags/assets information associated with aeroscout, client, rfid and/or zone.

Supported in the following platforms:

- Mobility RFS4000 Controller
- Mobility RFS6000 Controller
- Mobility RFS7000 Controller

Syntax

```
clear rtls tags[aeroscout|wireless-client|ekahau|rfid|zone
<1-48>]
```

Parameters

rtls tags [aeroscout |wireless-client|ekahau |rfid|zone <1-48>]	Real time locationing configuration
	• tags – Clears tag/asset information for:
	  • aeroscout – Clears Aeroscout tags
	  • g2 – Clear g2 tags
	  • wireless-client – Clears wireless-client(wi-fi clients)
	  • ekahau – Clears ekahau tags
	  • rfid – Clears passive RFID tags
	  • zone <1-48> – Clears tags in specified zone

Example

```
RFController(config-rtls)#clear rtls tags aeroscout
RFController(config-rtls)#
```

clrscr

RTLS config commands

Clears the display screen

Supported in the following platforms:

- Mobility RFS4000 Controller
- Mobility RFS6000 Controller
- Mobility RFS7000 Controller

Syntax

```
clrscr
```

Parameters

None

Example

```
RFController(config-rtls)#clrscr
RFController(config-rtls)#
```

end

RTLS config commands

Ends and exits the current mode and changes to the PRIV EXEC mode. The prompt changes to `RFController#`

Supported in the following platforms:

- Mobility RFS4000 Controller
- Mobility RFS6000 Controller
- Mobility RFS7000 Controller

Syntax

```
end
```

Parameters

None

Example

```
RFController(config-rtls)#end
RFController#
```

espi

RTLS config commands

Configures *Enterprise Services Programming Interface* (ESPI) related parameters

NOTE
espi command instantiates (config-rtls-espi) sub-instance. For more details see *ESPI Instance on page 729*. The prompt changes from RFController(config-rtls)# to RFController(config-rtls-espi)

Supported in the following platforms:

- Mobility RFS4000 Controller
- Mobility RFS6000 Controller
- Mobility RFS7000 Controller

Syntax

```
espi
```

Parameters

None

Example

```
RFController(config-rtls)espi
RFController(config-rtls-espi)
```

exit

RTLS config commands

Ends the current mode and moves to the previous mode (GLOBAL-CONFIG). The prompt changes to `RFController(config)#`

Supported in the following platforms:

- Mobility RFS4000 Controller
- Mobility RFS6000 Controller
- Mobility RFS7000 Controller

Syntax

```
exit
```

Parameters

None

Example

```
RFController(config-rtls)#exit
RFController(config)#
```

help

RTLS config commands

Displays the interactive help system for RTLS instance

Supported in the following platforms:

- Mobility RFS4000 Controller
- Mobility RFS6000 Controller
- Mobility RFS7000 Controller

Syntax

```
help
```

Parameters

None

Example

```
RFController(config-rtls)#help
CLI provides advanced help feature.  When you need help,
anytime at the command line please press '?'.

If nothing matches, the help list will be empty and you must backup
until entering a '?' shows the available options.
Two styles of help are provided:
1. Full help is available when you are ready to enter a
   command argument (e.g. 'show ?') and describes each possible
   argument.
2. Partial help is provided when an abbreviated argument is entered
   and you want to know what arguments match the input
   (e.g. 'show ve?'.)

RFController(config-rtls)#
```

ekahau

RTLS config commands

Enables and configures the external ekahau location engine

Supported in the following platforms:

- Mobility RFS4000 Controller
- Mobility RFS6000 Controller
- Mobility RFS7000 Controller

Syntax

```
ekahau [enable|engine ip<IP> port<Port>|multicast-listen-addr<MAC>]
```

Parameters

enable	Enables and configures external ekahau RTLS engine
engine ip<IP> port <Port>	Configures the IP address and port number of the external ekahau RTLS engine • ip – Configures external location engine IP address • port <1000-9000> – Configure external location engine port
multicast-listen-addr <MAC>	Configures multicast MAC address to which ekahau tags packets are destined • <MAC> – Multicast MAC address

Use `[no] enable` and `[no] engine <ip><port>` to undo theekahau RTLS engine configuration and disable it.

Example

```
RFController(config-rtls)#ekahau enable
RFController(config-rtls)#


RFController(config-rtls)#ekahau engine ip 10.1.1.1 port 1001
RFController(config-rtls)#

RFController(config-rtls)#ekahau multicast-listen-addr 01-18-8E-00-00-00
RFController(config-rtls)#
```

no

RTLS config commands

Negates a RTLS command or set its defaults

Supported in the following platforms:

- Mobility RFS4000 Controller
- Mobility RFS6000 Controller
- Mobility RFS7000 Controller

Syntax

```
no [aeroscout|ekahau|reference-tag|service|site|
controller|ap|zone]
```

Parameters

aeroscout [enable| multi-cast-listen|addr]	Negates aeroscout configuration • enable – Disable SOLE adapter • multicast-listen-addr– Configure multicast listening address
ekahau [enable|engine|multicast]	Negates ekahau configuration • enable – Disable aeroscout external engine • engine –reset external location engine parameters • multicast-listen-addr– Configure multicast listening address
reference-tag [rfid]	Negates reference-tag configuration • rfid– Negates configuring rfid tag
service [filter <1-100> {length| memory-bank|offset }|inventory {<1-100>|default]	Negates service configuration for: • filter <1-100> {length|memory-bank|offset} – Negates RFID tag filter configuration for the selected index • length – Length of tag filter • memory-bank – Tag memory bank • offset – Offset into the tag memory bank • inventory [<1-100>|default] – Negates tag inventory for the selected index or the default index • filter – Configures tag filter for inventory • start – Starts tag inventory • start-trigger – Removes start trigger for tag inventory • stop-trigger – Removes stop trigger for tag inventory • zone – Configures logical reader
site	Negates site configuration
zone<1-48>	Negates zone configuration
ap [MAC Address <coordinates>]	• AA-BB-CC-DD-EE-FF – Disables access point MAC IP address • coordinates – Negates AP location configuration
controller [coordinates |geo-coordinates]	• Negates controller configuration parameters • coordinates – Negates controller coordinates configuration within the site • geo-coordinates – Negates controller geo coordinates configuration

Usage Guidelines

Use `no` command to undo the configurations on the parameters mentioned in the table. Refer to the parameters, within this chapter, for complete syntax.

Example

```
RFController(config-rtls)#no aeroscout enable
RFController

RFController(config-rtls)#no ekahau enable
RFController(config-rtls)#

RFController(config-rtls)#no  ekahau engine
RFController(config-rtls)#

RFController(config-rtls)#no service inventory 1 zone 1
RFController(config-rtls)#
```

reference-tag

RTLS config commands

Configures fixed RFID tag as reference tag and sets its coordinates within a specified location

Supported in the following platforms:

- Mobility RFS4000 Controller
- Mobility RFS6000 Controller
- Mobility RFS7000 Controller

Syntax

```
reference-tag rfid <tag-id> coordinates x <0-65535> y
<0-65535> {[z<0-65535>]}{orientation [0|90|180|270]}
{range <1-50>}
```

Parameters

rfid <tag-id> coordinates x <0-65535> y <0-65535> {[z <0-65535>]} {orientation [0|90|180|270]} {range <1-50>}	Configures rfid tag as a reference tag • coordinates – Configures tag location • x <0-65535> – Configure X coordinate • y <0-65535> – Configure Y coordinate • z<0-65535> – Configure Y coordinate • orientation – Configures reference tag orientation (angles in degrees) • 0 – Increments only X • 90 – Decrements only X • 180 – Decrements only Y • 270 – Increments only Y • range <1-50> – Configures tag read range in feet.

Usage Guidelines

Use `[no] reference-tag rfid <tag-id> (coordinates x <0-65535> y <0-65535>) (orientation (0|90|180|270)) range <1-150>]` to rollback the reference-tag configuration.

Example

```
RFController(config-rtls)#reference-tag rfid Brocade coordinates x
600 y 600 orientation 180 range 40
RFController(config-rtls)#
```

rfid

RTLS config commands

Configures RFID reader parameters

Supported in the following platforms:

- Mobility RFS4000 Controller
- Mobility RFS6000 Controller
- Mobility RFS7000 Controller

NOTE
`rfid` command instantiates `(config-rtls-rfid)` sub-instance. For more details see *RFID Instance on page 739*. The prompt changes from `RFController(config-rtls)#` to `RFController(config-rtls-rfid)`

Syntax

```
rfid
```

Parameters

None

Example

```
RFController(config-rtls)#rfid
RFController(config-rtls-rfid)#
```

service

RTLS config commands

Invokes service commands to troubleshoot or debug `(config-rtls)` instance configurations

Supported in the following platforms:

- Mobility RFS4000 Controller
- Mobility RFS6000 Controller
- Mobility RFS7000 Controller

Syntax

```
service [filter|inventory|show]

service filter <1-100> [action|length|mask|
       memory-bank|name|offset]
        service filter <1-100> action [allow|deny]
    service filter <1-100> length <1-128>
service filter <1-100> mask <mask-name>
service filter <1-100> memory bank [epc|tid|uid]
service filter <1-100> name <name>
service filter <1-100> offset <0-32>

service inventory [<1-100>|default]
service inventory <1-100> [duration <0-100000>|
       filter{<1-100>|<name>}|report {current|differential}|
       round <0-10>|start|start-trigger|stop-trigger|zone]
service inventory <1-100> start-trigger [gpi port <1-65535>
       event <0-1> timeout <0-65535> |immediate|periodic
       offset <0-65535> period <0-65535> ]

service inventory <1-100> stop-trigger [duration
       <0-65535>|gpi port <1-65535> event <0-1> timeout <0-65535> |immediate]
service inventory <1-100> zone <1-48>

service show cli
```

Parameters

service filter <1-100> [action|length <1-128>|mask| memory-bank|name|offset<0-32>]	Configures RFID tag filter
	• action [allow|deny] – Configures action for tag filter. By default its configured to *allow*
	• length <1-128> – Configures number of bits to compare against tag mask
	• mask <name> – Configures tag mask for filter
	• memory-bank [epc|tid|uid] – Configures tag memory bank for the filter
	  • epc – EPC memory bank
	  • tid – TID memory bank
	  • uid – UID memory bank
	• name <name> – Configures tag filter name
	• offset <0-32> – Configures first location of memory bank against which the tag mask is compared

service inventory <1-100> [duration <0-100000>| filter{<1-100>|<name>}|report {current|differential}| round <0-10>|start| start-trigger|stop-trigger|zone]	A single tag inventory index
	• duration <0-100000> – Inventory period in msecs
	• filter [<1-100>|<name>] – Configures the selected tags filter for inventory.
	• report – Set tag inventory report type
	  • current – Reports current tag view
	  • differential – Reports only the tags changed since previous report
	• round <0-10> – Sets tag inventory round size
	• start – Starts tag inventory

	• start-trigger – Configures start trigger for tag inventory
	  • gpi – Configures GPI event based start trigger
	  • port <1-65535> – Configures GPI port number
	  • event <0-1> – Configures a boolean GPI event value that causes GPI event to trigger
	  • timeout <0-65535> – Configures trigger1 timeout in miliiseconds
	  • immediate – Starts tag inventory immediately
	  • periodic – Configures periodic tag inventory
	  • offset <0-65535> – Configures time offset in milliseconds
	  • period <0-65535> – Configures time period in milliseconds
	• stop-trigger – Configures stop trigger for tag inventory
	  • duration <0-65535> – Configures duration in milliseconds
	  • gpi – Configures GPI event based start trigger
	  • port <1-65535> – Configures GPI port number
	  • event <0-1> – Configures a boolean GPI event value that causes GPI event to trigger
	  • timeout <0-65535> – Configures trigger timeout in miliiseconds
	  • immediate – Stops tag inventory immediately
	• zone <1-48> – Configures the selected logical reader

show cli	Show running system information • cli – Show CLI tree of current mode

Usage Guidelines

Use `[no] service [options]` to rollback any service related configurations.

Example

```
RFController(config-rtls)#service filter 1 length 1
RFController(config-rtls)#
```

show

RTLS config commands

Displays current system information

Supported in the following platforms:

- Mobility RFS4000 Controller
- Mobility RFS6000 Controller
- Mobility RFS7000 Controller

Syntax

```
show <parameters>
show rtls [aeroscout|espi|filter|ekahau|reference-tags|
           rfid|site|sole|tags|zone]
```

Parameters

?	Suffix ? to the parameter to view its options and their related configuration details.

Usage Guidelines

Use ? at the end of each option until the final configuration is displayed.

Example

```
RFController(config-rtls)#show ?
  access-list           Internet Protocol (IP)
  aclstats              Show ACL Statistics information
  alarm-log             Display all alarms currently in the system
  autoinstall           autoinstall configuration
  banner                Display Message of the Day Login banner
  boot                  Display boot configuration.
  clock                 Display system clock
  commands              Show command lists
  crypto                encryption module
  debugging             Debugging information outputs
  dhcp                  DHCP Server Configuration
  environment           show environmental information
  file                  Display filesystem information
  firewall              Wireless firewall
  ftp                   Display FTP Server configuration
  history               Display the session command history
  interfaces            Interface status
  ip                    Internet Protocol (IP)
  ldap                  LDAP server
  licenses              Show any installed licenses
  logging               Show logging configuration and buffer
  mac                   Internet Protocol (IP)
  mac-address-table     Display MAC address table
  mac-name              Displays the configured MAC names
  management            Display L3 Managment Interface name
  mobility              Display Mobility parameters
  ntp                   Network time protocol
  password-encryption   password encryption
```

```
  port                  Physical/Aggregate port interface
  port-channel          Portchannel commands
  privilege             Show current privilege level
  protocol-list         List of protocols
  radius                RADIUS configuration commands
  role                  Configure role parameters
  redundancy            Display redundancy group parameters
  rtls                  Real Time Locating System commands
  running-config        Current Operating configuration
  securitymgr           Securitymgr parameters
  service-list          List of services
  sessions              Display current active open connections
  smtp-notifications     Display SNMP engine parameters
  snmp                  Display SNMP engine parameters
  snmp-server           Display SNMP engine parameters
  spanning-tree         Display spanning tree information
  startup-config        Contents of startup configuration
  static-channel-group  static channel group membership
  terminal              Display terminal configuration parameters
  timezone              Display timezone
  traffic-shape         Display traffic shaping
  upgrade-status        Display last image upgrade status
  users                 Display information about currently logged
                        in users
  version               Display software & hardware version
  virtual-ip            IP redundancy features
  wireless              Wireless configuration commands
  wlan-acl              wlan based acl

RFController(config-rtls)#show

RFController(config-rtls)#show rtls ?
  aeroscout       Aeroscout configurations
  espi            ESPI Configuration
  filter          RFID Tag Filters
  ekahau Ekahau configurations
  reference-tags  Reference tag Configurations
  rfid            RFID Configuration
  site            Site configurations
  sole            SOLE configurations
  tags            Tags/Assets (passive, active, wi-fi) Information
  zone            Show zone statistics

RFController(config-rtls)#show rtls

RFController(config-rtls)#show rtls site
Site Name              : Not configured
Site Description       : Not configured
Site Unit              : feet
Site Dimension         : 0L X 0W X 0H
Site Scale Factor      : 1.000000
Controller Coordinates     : 0:0:0
Swith Geo Coordinates  : Not configured
Number of APs          : 0
RFController(config-rtls)#
```

site

RTLS config commands

Configures RTLS site dimensions

Supported in the following platforms:

- Mobility RFS4000 Controller
- Mobility RFS6000 Controller
- Mobility RFS7000 Controller

Syntax

```
site [description|dimension|name|scale]
site description <description>
site dimension [unit [feet|meters]|x <1-9000> y <1-9000>
      z <0-180>]
site name <site-name>
site scale [<1-90>|auto]
```

Parameters

description <description>	Configures site description • <description> – Enter a description for the site

dimension [unit {feet|meters}|x <1-9000> y <1-9000> z <0-180>]	Configures site dimensions
	• length <value> – Configures site length. Select a value between <1-9000> if the unit is in feet, and if the unit is in meters the value will be between <1-3000>
	• width <value> – Configures width of the site. Select a value between <1-9000> if the unit is in feet, and if the unit is in meters the value will be between <1-3000>.
	• height <value> – Configures height of the site. Select a value between <0-180>, if the unit is in feet and if the unit is in meters the value will be between <0-60>unit – Configures the distance measurement unit to be used for the site
	  • feet – Site distances measured in feet
	  • meters – Site distances measured in meters

name <site-name>	Configures name for the site
scale [<1-90>|auto]	Configures site scale • <1-90> - Configures scale value ranging between 1 - 90 • auto - Auto configures scale

Usage Guidelines

Use `[no] site [description |dimension|name]` to rollback the configurations made using the `site` command

Example

```
RFController(config-rtls)#site description "Brocade RMZ Ecospace,
India, 5th Floor"
RFController(config-rtls)#

RFController(config-rtls)#site name "BLR-RMZ Ecospace"
RFController(config-rtls)#
```

sole

RTLS config commands

Sets *Smart Opportunistic Location Engine* (SOLE) related configuration commands

This command leads you to the `(config-rtls-sole)#` sub-instance.

Supported in the following platforms:

- Mobility RFS4000 Controller
- Mobility RFS6000 Controller
- Mobility RFS7000 Controller

NOTE
`sole` command instantiates `(config-rtls-sole)` sub-instance. For more details see *SOLE Instance on page 753*. The prompt changes from `RFController(config-rtls)#` to `RFController(config-rtls-sole)`

Syntax

```
sole
```

Parameters

None

Example

```
RFController(config-rtls)#sole
RFController(config-rtls-sole)#
```

controller

RTLS config commands

Configures the controller's geographical location parameters

Supported in the following platforms:

- Mobility RFS4000 Controller
- Mobility RFS6000 Controller
- Mobility RFS7000 Controller

Syntax

```
controller [coordinates|geo-coordinates]
controller coordinates x <0-65535> y <0-65535> z <0-65535>
controller geo-coordinates longitude <-180.00-80.00>
       latitude <-90.00 - 90.00>
```

Parameters

coordinates x <0-65535> y <0-65535> z <0-65535>	Configures controller coordinates within the site • x <0-65535> – Configures X coordinate • y <0-65535> – Configures Y coordinate • z <0-65535> – Configures Z coordinate
longitude <-180.00-80.00> latitude <-90.00 - 90.00>	Configures controller geographic coordinates • longitude <-180.00-180.00> – Configures longitude in degrees • latitude <-90.00-90.00> – Configures latitude in degrees

Example

```
RFController(config-rtls)#controller coordinates x 121 y 121 z 135
RFController(config-rtls)#

RFController(config-rtls)#controller geo-coordinates longitude 120 latitude 70
RFController(config-rtls)#
```

zone

RTLS config commands

Configures the zone. Maximum of 16 zones can be configured for a site.

Supported in the following platforms:

- Mobility RFS4000 Controller
- Mobility RFS6000 Controller
- Mobility RFS7000 Controller

Syntax

```
zone <1-48> [name <name>|perimeter x <0-65535> y <<0-65535> ]
```

Parameters

<1-48>name <name>|perimeter x <0-65535> y <<0-65535>]	Select a single zone index for configuration
	• name <name> – Configures name of new zone
	• perimeter [x y]– Configures zone perimeter coordinates
	  • x <0-65535> – Defines X coordinate
	  • y <0-65535> – Defines Y coordinate

Usage Guidelines

Use **{no} zone <index> [options]** to negate a zones configurations

Example

```
RFController(config-rtls)#zone 1 name yard
RFController(config-rtls)#

RFController(config-rtls)#zone 1 perimeter x 0 y 0
RFController(config-rtls)#

RFController(config-rtls)#zone 1 perimeter x 40 y 0
RFController(config-rtls)#

RFController(config-rtls)#zone 1 perimeter x 40 y 100
```

ap

RTLS config commands

Supported in the following platforms:

- Mobility RFS4000 Controller
- Mobility RFS6000 Controller
- Mobility RFS7000 Controller

Syntax

```
ap <MAC> coordinates x <0-9000> y <0-9000>
       z <0-180>
```

Parameters

<MAC> coordinates x <0-9000> y <0-9000> z <0-180>	Select a single zone index for configuration
	• <MAC> – Configures access point MAC Address
	  • x <0-9000> – Defines X coordinate
	  • y <0-9000> – Defines Y coordinate
	  • z <0-180> – Defines Z coordinate

Example

```
RFController(config-rtls)#ap AA-BB-CC-DD-EE-FF x 10 y 10 z 0
RFController(config-rtls)#
```

Chapter

ESPI Instance

22

In this chapter

Use the `(config-rtls-espi)` instance to configure *Enterprise Services Programming Interface* (ESPI) related configuration commands.

To navigate to this instance, use the commands

```
RFController(config)#rtls
RFController(config-rtls)#espi
RFController(config-rtls-espi)#
```

ESPI config commands

Table 24 summarizes **`config-rtls-espi`** commands:

TABLE 24 ESPI Config Command Summary

Command	Description	Ref.
adapter	Adapters configurations	*page 730*
clrscr	Clears the display screen	*page 731*
end	Ends the current mode and changes to the EXEC mode	*page 732*
exit	End the current mode and moves to the previous mode	*page 733*
help	Describes the interactive help system	*page 734*
no	Negates a command or set its defaults	*page 735*
service	Service Commands	*page 736*
show	Shows running system information	*page 737*

adapter

ESPI config commands

Enables/disables a specified adapter or all adapters

Supported in the following platforms:

- Mobility RFS4000 Controller
- Mobility RFS6000 Controller
- Mobility RFS7000 Controller

Syntax

```
adapter ale-tcp [enable|port <3000-3100>]
```

Parameters

adapter ale-tcp [enable|port <3000-3100>]	Application side protocol implemented by adapter.
	• ale-tcp – ALE over TCP Adapter
	  • enable – Activates/enables ESPI adapter
	  • port <3000-3100> – Configures ESPI adapter listening port

Usage Guidelines

Use **{no} adapter <adapter> enable** to disable the specified adapter

NOTE
ALE-TCP is the only adapter shipped along with the controller.

Example

```
RFController(config-rtls-espi)#adapter ale-tcp port 3040
RFController(config-rtls-espi)#
```

clrscr

ESPI config commands

Clears the display screen

Supported in the following platforms:

- Mobility RFS4000 Controller
- Mobility RFS6000 Controller
- Mobility RFS7000 Controller

Syntax

```
clrscr
```

Parameters

None

Example

```
RFController(config-rtls-espi)#clrscr
RFController(config-rtls-espi)#
```

end

ESPI config commands

Ends and exits the current mode and moves to the PRIV EXEC mode. The prompt changes to `RFController#`

Supported in the following platforms:

- Mobility RFS4000 Controller
- Mobility RFS6000 Controller
- Mobility RFS7000 Controller

Syntax

```
end
```

Parameters

None

Example

```
RFController(config-rtls-espi)#end
RFController#
```

exit

ESPI config commands

Ends the current mode and moves to the previous mode (GLOBAL-CONFIG). The prompt changes to `RFController(config)#`

Supported in the following platforms:

- Mobility RFS4000 Controller
- Mobility RFS6000 Controller
- Mobility RFS7000 Controller

Syntax

```
exit
```

Parameters

None

Example

```
RFController(config-rtls-espi)#exit
RFController(config)#
```

help

ESPI config commands

Displays the system's interactive help in HTML format

Supported in the following platforms:

- Mobility RFS4000 Controller
- Mobility RFS6000 Controller
- Mobility RFS7000 Controller

Syntax

```
help
```

Parameters

None

Example

```
RFController(config-rtls-espi)#help
CLI provides advanced help feature.  When you need help,
anytime at the command line please press '?'.

If nothing matches, the help list will be empty and you must backup
until entering a '?' shows the available options.
Two styles of help are provided:
1. Full help is available when you are ready to enter a
   command argument (e.g. 'show ?') and describes each possible
   argument.
2. Partial help is provided when an abbreviated argument is entered
   and you want to know what arguments match the input
   (e.g. 'show ve?'.)

RFController(config-rtls-espi)#
```

no

ESPI config commands

Defines the name of the adapter or disables the adapter(s)

Supported in the following platforms:

- Mobility RFS4000 Controller
- Mobility RFS6000 Controller
- Mobility RFS7000 Controller

Syntax

```
no adapter ale-tcp [enable|port <3000-3100>]
```

Parameters

adapter ale-tcp [enable|port <3000-3100>]	Negates ESPI adapter configurations.
	• adapter – Application side Protocol implemented by adapter.
	  • ale-tcp – ALE over TCP Adapter
	  • enable – Deactivates/disables ESPI adapter
	  • port <3000-3100>– Configure ESPI adapter listening port

Example

```
RFController(config-rtls-espi)#no adapter ale-tcp enable
RFController(config-rtls-espi)#
```

service

ESPI config commands

Invokes service commands to troubleshoot or debug `(config-if)` instance configurations

Supported in the following platforms:

- Mobility RFS4000 Controller
- Mobility RFS6000 Controller
- Mobility RFS7000 Controller

Syntax

```
service show cli
```

Parameters

None

Example

```
RFController(config-rtls-espi)#service show cli
ESPI Config mode:
+-adapter
  +-ADAPTER
    +-activate [adapter ADAPTER activate]
    +-port
      +-<3000-3100> [adapter ADAPTER port <3000-3100>]
+-clrscr [clrscr]
+-do
  +-LINE [do LINE]
+-end [end]
+-exit [exit]
+-help [help]
+-no
  +-adapter
    +-ADAPTER
      +-activate [no adapter ADAPTER activate]
+-quit [quit]
.....................................................................
.....................................................................
.....................................................................
.....................................................................
.....................................................................
.................
RFController(config-rtls-espi)#
```

show

ESPI config commands

Displays current system information

Supported in the following platforms:

- Mobility RFS4000 Controller
- Mobility RFS6000 Controller
- Mobility RFS7000 Controller

Syntax

```
show <parameters>
```

Parameters

?	Displays the parameters for which information can be viewed using the show command

Example

```
RFController(config-rtls-espi)#show ?
  access-list            Internet Protocol (IP)
  aclstats               Show ACL Statistics information
  alarm-log              Display all alarms currently in the system
  autoinstall            autoinstall configuration
  banner                 Display Message of the Day Login banner
  boot                   Display boot configuration.
  clock                  Display system clock
  commands               Show command lists
  crypto                 encryption module
  debugging              Debugging information outputs
  dhcp                   DHCP Server Configuration
  environment            show environmental information
  file                   Display filesystem information
  firewall               Wireless firewall
  ftp                    Display FTP Server configuration
  history                Display the session command history
  interfaces             Interface status
  ip                     Internet Protocol (IP)
  ldap                   LDAP server
  licenses               Show any installed licenses
  logging                Show logging configuration and buffer
  mac                    Internet Protocol (IP)
  mac-address-table      Display MAC address table
  mac-name               Displays the configured MAC names
  management             Display L3 Managment Interface name
  mobility               Display Mobility parameters
  ntp                    Network time protocol
  password-encryption    password encryption
  port                   Physical/Aggregate port interface
  port-channel           Portchannel commands
  privilege              Show current privilege level
  protocol-list          List of protocols
  radius                 RADIUS configuration commands
  role                   Configure role parameters
  redundancy             Display redundancy group parameters
  rtls                   Real Time Locating System commands
```

```
  running-config        Current Operating configuration
  securitymgr           Securitymgr parameters
  service-list          List of services
  sessions              Display current active open connections
  smtp-notification     Display SNMP engine parameters
  snmp                  Display SNMP engine parameters
  snmp-server           Display SNMP engine parameters
  spanning-tree         Display spanning tree information
  startup-config        Contents of startup configuration
  static-channel-group  static channel group membership
  terminal              Display terminal configuration parameters
  timezone              Display timezone
  traffic-shape         Display traffic shaping
  virtual-ip            IP redundancy feature
  upgrade-status        Display last image upgrade status
  users                 Display information about currently logged
                        in users
  version               Display software & hardware version
  virtual-ip            IP redundancy feature
  wireless              Wireless configuration commands
  wlan-acl              wlan based acl

RFController(config-rtls-espi)#show

RFController(config-rtls-espi)#show rtls espi ?
  adapter     Adapter Configuration
  ecspecs     ECSpecs configuration
  subscriber  Show info for giver subsriber's IP
  tags        Tags/Assets (passive, active, wi-fi, uwb) Information

RFController(config-rtls-espi)#show rtls espi
```

Chapter

RFID Instance

23

In this chapter

The `(config-rtls-rfid)` instance is used to configure RFID reader related configuration parameters.

To navigate to this instance, use the commands

```
RFController(config)#rtls
RFController(config-rtls)#rfid
RFController(config-rtls-rfid)#
```

RFID config commands

Table 25 summarizes **`config-rtls-rfid`** commands:

TABLE 25 RFID Config Commands

Command	Description	Ref.
activate	Activates/enables RFID reader configuration	*page 740*
clrscr	Clears the display screen	*page 741*
end	Ends the current mode and moves to EXEC mode	*page 742*
exit	Ends current mode and moves to the previous mode	*page 743*
help	Description of the interactive help system	*page 744*
no	Negates a command or set its defaults	*page 745*
reader	RFID Readers configuration commands	*page 746*
service	Invokes service commands to troubleshoot or debug `(config-rtls)` instance configurations	*page 748*
show	Displays the running system information	*page 751*

activate

RFID config commands

Activates and enables the *Real Time Location System* (RTLS) adapter

Supported in the following platforms:

- Mobility RFS4000 Controller
- Mobility RFS6000 Controller
- Mobility RFS7000 Controller

Syntax

```
activate
```

Parameters

None

Usage Guidelines

Use [no] to disable and deactivate the RTLS adapter

Example

```
RFController(config-rtls-rfid)#activate
RFController(config-rtls-rfid)#
```

clrscr

RFID config commands

Clears the display screen

Supported in the following platforms:

- Mobility RFS4000 Controller
- Mobility RFS6000 Controller
- Mobility RFS7000 Controller

Syntax

```
clrscr
```

Parameters

None

Example

```
RFController(config-rtls-rfid)#clrscr
RFController(config-rtls-rfid)#
```

end

RFID config commands

Ends and exits the current mode and changes to the PRIV EXEC mode. The prompt changes to `RFController#`

Supported in the following platforms:

- Mobility RFS4000 Controller
- Mobility RFS6000 Controller
- Mobility RFS7000 Controller

Syntax

```
end
```

Parameters

None

Example

```
RFController(config-rtls-rfid)#end
RFController#
```

exit

RFID config commands

Ends the current mode and moves to the previous mode (GLOBAL-CONFIG). The prompt changes to `RFController(config)#`

Supported in the following platforms:

- Mobility RFS4000 Controller
- Mobility RFS6000 Controller
- Mobility RFS7000 Controller

Syntax

```
exit
```

Parameters

None

Example

```
RFController(config-rtls-rfid)#exit
RFController(config-rtls)#
```

help

RFID config commands

Displays the interactive help system for RTLS instance

Supported in the following platforms:

- Mobility RFS4000 Controller
- Mobility RFS6000 Controller
- Mobility RFS7000 Controller

Syntax

```
help
```

Parameters

None

Example

```
RFController(config-rtls-rfid)#help
CLI provides advanced help feature.  When you need help,
anytime at the command line please press '?'.

If nothing matches, the help list will be empty and you must backup
until entering a '?' shows the available options.
Two styles of help are provided:
1. Full help is available when you are ready to enter a
   command argument (e.g. 'show ?') and describes each possible
   argument.
2. Partial help is provided when an abbreviated argument is entered
   and you want to know what arguments match the input
   (e.g. 'show ve?'.)

RFController(config-rtls-rfid)#
```

no

RFID config commands

Supported in the following platforms:

- Mobility RFS4000 Controller
- Mobility RFS6000 Controller
- Mobility RFS7000 Controller

Syntax

```
no [activate|reader|service]
```

Parameters

activate	Deactivates/disables RTLS adapter
reader	Disables RFID reader configuration commands
service	Disables service commands

Usage Guidelines

Use `[no]` command to undo the configurations on the parameters mentioned in the table. Refer to the parameters, within this chapter, for complete syntax.

Example

```
RFController(config-rtls-rfid)#no activate
RFController(config-rtls-rfid)#
```

reader

RFID config commands

Configures RFID Readers parameters

Supported in the following platforms:

- Mobility RFS4000 Controller
- Mobility RFS6000 Controller
- Mobility RFS7000 Controller

Syntax

```
reader [<index>|<reader-index-list>]

reader <index> [antenna|coordinates|description|
       enable|id|name]
reader <index> antenna [<antenna>|<antenna-list>]
reader <index> antenna <antenna-list> [coordinates x
       <x-coordinate> y <y-coordinate> z <z-coordinate>|
       power <antenna-power>]
reader <index> coordinates x <x-coordinate> y <y-coordinate>
       z <z-coordinate>
reader [<index>|<reader-index-list>] id <ip>
reader [<index>|<reader-index-list>] description
       <description>
reader [<index>|<reader-index-list>] enable
reader [<index>|<reader-index-list>] name <name>
```

Parameters

reader [<index>|<reader-index-list>]	Enter a single RFID reader index or a list (1,3,7) or range (3-7) of RFID reader indices
antenna [<antenna>|<antenna-list>] coordinates x <x-coordinate> y <y-coordinate> *z* <*z-coordinate*>	Configures the RFID readers antenna. Select a antenna using its index, between <1-8> or range (eg:3-7) of antenna indices or any RFID reader antenna • coordinates - Sets the coordinates for the antenna • x <x-coordinate> – Configures the x coordinate for the antenna for the RFID reader. • y <y-coordinate> – Configures the y coordinate for the antenna for the RFID reader. • z <z-coordinate> – Configures the z coordinate for the antenna for the RFID reader.
reader [<index>|<reader-index-list>] antenna [<antenna>|<antenna-list>] power <antenna-power>	Configures the RFID reader power. • power – Sets the power • <antenna-power> – Sets the antenna power to between <-63 and 63 dBm.
reader <index> id <ip>	Sets the IP address <ip> for the reader with index <index>.
reader <index> coordinates x <x-coordinate> y <y-coordinate> *z* <*z-coordinate*>	Sets the coordinates for the RFID reader. • coordinates - Sets the coordinates for the reader • x <x-coordinate> – Configures the x coordinate for the RFID reader. • y <y-coordinate> – Configures the y coordinate for the RFID reader. • z <z-coordinate> – Configures the z coordinate for the RFID reader.
reader [<index>|<reader-index-list>] description <description>	Sets the description of a RFID reader or a list of readers to <description> (1-32 characters).
reader [<index>|<reader-index-list>] enable	Enables or connects the RFID reader with the index <index> or a list of RFID readers <reader-index-list>.
reader [<index>|<reader-index-list>] name <name>	Sets a user friendly name to a RFID reader or a group of RFID readers to <name> (1-20 characters).

Usage Guidelines

Use `[no] reader [<index>|<range>][options]` to rollback any configurations performed using the `reader` command

Example

```
RFController(config-rtls-rfid)#reader 1 antenna 1 coordinates x 400 y 400 z
500
RFController(config-rtls-rfid)#
```

service

RFID config commands

Invokes service commands to troubleshoot or debug (config-if) instance configurations

Supported in the following platforms:

- Mobility RFS4000 Controller
- Mobility RFS6000 Controller
- Mobility RFS7000 Controller

Syntax

```
service show cli
service reader [<reader-index>|<reader-index-list>] [antenna|upgrade]

service reader [<reader-index>|<reader-index-list>] antenna
[<antenna-index>|<antenna-list>|any] filter
[<tag-filter-index>|<tag-filter-name>]

service reader [<reader-index>|<reader-index-list>] upgrade ipaddr <ftp-ip>
ftp-username <ftp-username> ftp-password <ftp-password> ftp-path <file-path>
username <reader-admin-username> password <reader-admin-password>
```

Parameters

show cli	Displays the CLI tree of the current mode

service reader [<reader-index>|<reader-index-list>] antenna [<antenna-index>|<antenna-list>|any] filter [<tag-filter-index>|<tag-filter-name>]	Displays the RFID reader configuration information.
	• <reader-index> – The RFID reader index.
	• <reader-index-list> – A list of comma separated RFID reader indices.
	• antenna [<antenna-index>|<antenna-list>|all] – The antenna information.
	  • <antenna-index> – The antenna index in case of readers with multiple antennae.
	  • <antenna-list> – The list of comma separated antenna indices.
	  • any – Indicates all antennas.
	• filter [<tag-filter-index>|<tag-filter-name>] – RFID Tag filter configuration
	  • <tag-filter-index> – The index of the Tag Filter.
	  • <tag-filter-name> – The name of the Tag Filter.

service reader [<reader-index>|<reader-index-list>] upgrade ipaddr <ftp-ip> ftp-username <ftp-username> ftp-password <ftp-password> ftp-path <file-path> username <reader-admin-username> password <reader-administrative-password>	Upgrades the RFID readers. • <reader-index> – The RFID reader index. • <reader-index-list> – A list of comma separated RFID reader indices. • upgrade ipaddr <ftp-ip> – Upgrades the selected RFID reader/readers from the ip address <ftp-ip> • ftp-username <ftp-username> – The ftp username for the upgrade FTP server. • ftp-password <ftp-password> – The password for the ftp-username <ftp-username>. • ftp-path <file-path> – The path to the upgrade file on the FTP server. • username <reader-admin-username> – The administrative username on the reader. • password <reader-admin-password> – The password for the username <reader-admin-username>.

Example

```
RFController(config-rtls-rfid)#service show cli
RFID readers Config mode:
+-activate [activate]
+-adopt-unconf-readers [adopt-unconf-readers]
+-clrscr [clrscr]
+-do
  +-LINE [do LINE]
+-end [end]
+-exit [exit]
+-help [help]
+-no
  +-activate [no activate]
  +-adopt-unconf-readers [no adopt-unconf-readers]
  +-reader
    +-<1-48>
      +-antenna
        +-<1-8>
          +-coordinates [no reader (<1-48>|READER) antenna (<1-8>|ANTENNA)
coordinates]
```

```
          +-filter [no reader (<1-48>|READER) antenna
(<1-.....................................................................
.....................................................................
.....................................................................
.....................................................................
RFController(config-rtls-rfid)#
```

show

RFID config commands

Displays current system information

Supported in the following platforms:

- Mobility RFS4000 Controller
- Mobility RFS6000 Controller
- Mobility RFS7000 Controller

Syntax

```
show <parameter>
```

Parameters

?	Displays the parameters for which information can be viewed using the show command

Example

```
RFController(config-rtls-rfid)#show ?
  access-list           Internet Protocol (IP)
  aclstats              Show ACL Statistics information
  alarm-log             Display all alarms currently in the system
  autoinstall           autoinstall configuration
  banner                Display Message of the Day Login banner
  boot                  Display boot configuration.
  clock                 Display system clock
  commands              Show command lists
  crypto                encryption module
  debugging             Debugging information outputs
  dhcp                  DHCP Server Configuration
  environment           show environmental information
  file                  Display filesystem information
  firewall              Wireless firewall
  ftp                   Display FTP Server configuration
  history               Display the session command history
  interfaces            Interface status
  ip                    Internet Protocol (IP)
  ldap                  LDAP server
  licenses              Show any installed licenses
  logging               Show logging configuration and buffer
  mac                   Internet Protocol (IP)
  mac-address-table     Display MAC address table
  mac-name              Displays the configured MAC names
  management            Display L3 Managment Interface name
  mobility              Display Mobility parameters
  ntp                   Network time protocol
  password-encryption   password encryption
  port                  Physical/Aggregate port interface
  port-channel          Portchannel commands
  privilege             Show current privilege level
  protocol-list         List of protocols
  radius                RADIUS configuration commands
  role                  Configure role parameters
  redundancy            Display redundancy group parameters
  rtls                  Real Time Locating System commands
```

```
  running-config        Current Operating configuration
  securitymgr           Securitymgr parameters
  service-list          List of services
  sessions              Display current active open connections
  smtp-notification     Display SNMP engine parameters
  snmp                  Display SNMP engine parameters
  snmp-server           Display SNMP engine parameters
  spanning-tree         Display spanning tree information
  startup-config        Contents of startup configuration
  static-channel-group  static channel group membership
  terminal              Display terminal configuration parameters
  timezone              Display timezone
  traffic-shape         Display traffic shaping
  virtual-ip            IP redundancy feature
  upgrade-status        Display last image upgrade status
  users                 Display information about currently logged
                        in users
  version               Display software & hardware version
  virtual-ip            IP redundancy feature
  wireless              Wireless configuration commands
  wlan-acl              wlan based acl

RFController(config-rtls-rfid)#show

RFController(config-rtls-rfid)#show rtls rfid ?
  LLRP       Reader protocol statistics (LLRP)
  inventory  RFID Tag Inventory
  reader     RFID Reader configuration commands
RFController(config-rtls-rfid)#
```

Chapter

SOLE Instance

24

In this chapter

Use the `(config-rtls-sole)` instance to configure SOLE Location Engine related parameters.

To navigate to this instance, use the commands

```
RFController(config)#rtls
RFController(config-rtls)#sole
RFController(config-rtls-sole)#
```

SOLE config commands

Table 26 summarizes `config-rtls-sole` commands:

TABLE 26 Location Engine Config Command Summary

Command	Description	Ref.
clrscr	Clears the display screen	*page 754*
end	Ends the current mode and moves to EXEC mode	*page 755*
exit	Ends current mode and moves to the previous mode	*page 756*
help	Description of the interactive help system	*page 757*
locate	Configures location commands	*page 758*
no	Negates a command or set its defaults	*page 759*
redundancy	Enables redundancy support across cluster members for SOLE	*page 760*
service	Invokes service commands to troubleshoot or debug `(config-rtls)` instance configurations	*page 761*
show	Displays the running system information	*page 762*
rssi-filter	Filters rssi value in dbm	*page 764*
aap-rssi-updat e-interval	Displays AAP probe packet interval value in seconds	*page 765*
wireless-client	Displays wireless-client configurations	*page 766*

clrscr

SOLE config commands

Clears the display screen

Supported in the following platforms:

- Mobility RFS4000 Controller
- Mobility RFS6000 Controller
- Mobility RFS7000 Controller

Syntax

```
clrscr
```

Parameters

None

Example

```
RFController(config-rtls-sole)#clrscr
RFController(config-rtls-sole)#
```

end

SOLE config commands

Ends and exits the current mode and changes to the PRIV EXEC mode. The prompt changes to `RFController#`

Supported in the following platforms:

- Mobility RFS4000 Controller
- Mobility RFS6000 Controller
- Mobility RFS7000 Controller

Syntax

```
end
```

Parameters

None

Example

```
RFController(config-rtls-sole)#end
RFController#
```

exit

SOLE config commands

Ends the current mode and moves to the previous mode (GLOBAL-CONFIG). The prompt changes to `RFController(config)#`

Supported in the following platforms:

- Mobility RFS4000 Controller
- Mobility RFS6000 Controller
- Mobility RFS7000 Controller

Syntax

```
exit
```

Parameters

None

Example

```
RFController(config-rtls-sole)#exit
RFController(config-rtls-sole)#
```

help

SOLE config commands

Displays the interactive help system for RTLS instance

Supported in the following platforms:

- Mobility RFS4000 Controller
- Mobility RFS6000 Controller
- Mobility RFS7000 Controller

Syntax

```
help
```

Parameters

None

Example

```
RFController(config-rtls-sole)#help
CLI provides advanced help feature.  When you need help,
anytime at the command line please press '?'.

If nothing matches, the help list will be empty and you must backup
until entering a '?' shows the available options.
Two styles of help are provided:
1. Full help is available when you are ready to enter a
   command argument (e.g. 'show ?') and describes each possible
   argument.
2. Partial help is provided when an abbreviated argument is entered
   and you want to know what arguments match the input
   (e.g. 'show ve?'.)

RFController(config-rtls-sole)#
```

locate

SOLE config commands

Configures location commands

Supported in the following platforms:

- Mobility RFS4000 Controller
- Mobility RFS6000 Controller
- Mobility RFS7000 Controller

Syntax

```
locate [aeroscout|wireless-client|ekahau]
locate wireless-client [<MAC-Addr>|enable|interval]
locate ekahau [enable|interval]
```

Parameters

aeroscout [enable|interval <5-3600>	Locates aeroscout tags • enable – Enables on-board aeroscout location engine service • interval <5-3600> – Configures location interval for on-board locationing of aeroscout tags in seconds
wireless-client [<MAC-Addr>| enable|interva <5-3600>l]	Locates specified wireless client • <MAC-Addr> enable – Enables location of specified Client • enable – Enables location of all specified clients • interval <5-3600> – Configures clients location interval for locationing of clients in seconds **NOTE:** The controller currently supports locationing of 512 clients only.
ekahau [enable| interval<5-3600>	Locates ekahau tags • enable – Enables on-board locationing of`ekahau` tags • interval <5-3600> – Configures location interval for on-board locationing of ekahau tags in seconds

Usage Guidelines

Use `[no] locate [aeroscout|wireless-client|ekahau]` to rollback and disable all the configurations performed using `locate` command

Example

```
RFController(config-rtls-sole)#locate aeroscout enable
RFController(config-rtls-sole)#

RFController(config-rtls-sole)#locate aeroscout interval 300
RFController(config-rtls-sole)#
```

no

SOLE config commands

Disables the locationing adapter(s) and its configurations

Supported in the following platforms:

- Mobility RFS4000 Controller
- Mobility RFS6000 Controller
- Mobility RFS7000 Controller

Syntax

```
no [aap-rssi-update-interval|locate|mobile-nit|redundancy|
rssi-filter]
```

Parameters

aap-rssi-update-interval	Disables AAP probe packet interval
locate [aeroscout|ekahau|wireless-client]	Negates Location commands
wireless-client [<MAC-Addr|enable|interval <5-3600>]	Locates specified wireless-client • <MAC-Addr> (enable) – Disables location of specified mobile unit • enable – Disables location of all specified wireless clients • interval <5-3600> – Resets the location interval for the locationing of clients
redundancy enable	Disables SOLE redundancy
rssi-filter	Disables rssi-filter value in dbm

Example

```
RFController(config-rtls-sole)#no locate wireless-client enable
RFController(config-rtls-sole)#

RFController(config-rtls-sole)#no locate wireless-client interval
RFController(config-rtls-sole)#
```

redundancy

SOLE config commands

Enables redundancy support across cluster members for SOLE

Supported in the following platforms:

- Mobility RFS4000 Controller
- Mobility RFS6000 Controller
- Mobility RFS7000 Controller

Syntax

```
redundancy enable
```

Parameterse

redundancy enable	Enables the redundancy support across cluster members for SOLE

Usage Guidelines

This command is disabled by default

Example

```
RFController(config-rtls-sole)#redundancy enable
RFController(config-rtls-sole)#
```

service

SOLE config commands

Invokes service commands to troubleshoot or debug `(config-rtls)` instance configurations

Supported in the following platforms:

- Mobility RFS4000 Controller
- Mobility RFS6000 Controller
- Mobility RFS7000 Controller

Syntax

```
service show cli
```

Parameters

None

Example

```
RFController(config-rtls-sole)#service show cli
Location Engine Config mode:
+-clrscr [clrscr]
+-end [end]
+-exit [exit]
+-help [help]
+-locate
  +-aeroscout
    +-enable [locate (aeroscout|ekahau) (interval <5-3600>|enable)]
    +-interval
      +-<5-3600> [locate (aeroscout|ekahau) (interval <5-3600>|enable)]
  +-wireless-client
    +-AA-BB-CC-DD-EE-FF
      +-enable [locate wireless-client (AA-BB-CC-DD-EE-FF|) enable]
    +-enable [locate wireless-client (AA-BB-CC-DD-EE-FF|) enable]
    +-interval
      +-<5-3600> [locate wireless-client interval <5-3600>]
  +-ekahau
    +-enable [locate (aeroscout|ekahau) (interval <5-3600>|enable)]
    +-interval.........................
RFController(config-rtls-sole)#
```

show

SOLE config commands

Displays current system information

Supported in the following platforms:

- Mobility RFS4000 Controller
- Mobility RFS6000 Controller
- Mobility RFS7000 Controller

Syntax

```
show <parameters>
```

Parameters

?	Displays the parameters for which information can be viewed using the show command

Example

```
RFController(config-rtls-sole)#show ?
  access-list           Internet Protocol (IP)
  aclstats              Show ACL Statistics information
  alarm-log             Display all alarms currently in the system
  autoinstall           autoinstall configuration
  banner                Display Message of the Day Login banner
  boot                  Display boot configuration.
  clock                 Display system clock
  commands              Show command lists
  crypto                encryption module
  debugging             Debugging information outputs
  dhcp                  DHCP Server Configuration
  environment           show environmental information
  file                  Display filesystem information
  firewall              Wireless firewall
  ftp                   Display FTP Server configuration
  history               Display the session command history
  interfaces            Interface status
  ip                    Internet Protocol (IP)
  ldap                  LDAP server
  licenses              Show any installed licenses
  logging               Show logging configuration and buffer
  mac                   Internet Protocol (IP)
  mac-address-table     Display MAC address table
  mac-name              Displays the configured MAC names
  management            Display L3 Managment Interface name
  mobility              Display Mobility parameters
  ntp                   Network time protocol
  password-encryption   password encryption
  port                  Physical/Aggregate port interface
  port-channel          Portchannel commands
  privilege             Show current privilege level
  protocol-list         List of protocols
  radius                RADIUS configuration commands
  role                  Configure role parameters
  redundancy            Display redundancy group parameters
```

```
  rtls                  Real Time Locating System commands
  running-config        Current Operating configuration
  securitymgr           Securitymgr parameters
  service-list          List of services
  sessions              Display current active open connections
  smtp-notification     Display SNMP engine parameters
  snmp                  Display SNMP engine parameters
  snmp-server           Display SNMP engine parameters
  spanning-tree         Display spanning tree information
  startup-config        Contents of startup configuration
  static-channel-group  static channel group membership
  terminal              Display terminal configuration parameters
  timezone              Display timezone
  traffic-shape         Display traffic shaping
  upgrade-status        Display last image upgrade status
  users                 Display information about currently logged
                        in users
  version               Display software & hardware version
  virtual-ip            IP redundancy feature
  wireless              Wireless configuration commands
  wlan-acl              wlan based acl

RFController(config-rtls-sole)#show

RFController(config-rtls-sole)#show rtls sole ?
  peers   Show SOLE peer information
  probes  Show probe information
RFController(config-rtls-sole)#

RFController(config-rtls-sole)#show rtls sole peers
SOLE-WCCP status    :DOWN
SOLE-WCCP IP address:0.0.0.0
SOLE-Peer count     :0
RFController(config-rtls-sole)#

RFController(config-rtls-sole)#show rtls sole probes
  #    Tag MAC             Type         Controller-Id  Probes  Time
RFController(config-rtls-sole)#
```

rssi-filter

SOLE config commands

Filters rssi values below this threshold

Supported in the following platforms:

- Mobility RFS4000 Controller
- Mobility RFS6000 Controller
- Mobility RFS7000 Controller

Syntax

```
rssi-filter <-100-0>
```

Parameters

<-100-0>	Displays rssi filter value in dbm

Example

```
RFController(config-rtls-sole)#rssi-filter -9
RFController(config-rtls-sole)#
```

aap-rssi-update-interval

SOLE config commands

Displays AAP probe packet interval value in seconds

Supported in the following platforms:

- Mobility RFS4000 Controller
- Mobility RFS6000 Controller
- Mobility RFS7000 Controller

Syntax

```
aap-rssi-update-interval <5-3600>
```

Parameters

aap-rssi-update-interval <5-3600>	Displays aap-rssi filter value in seconds

Example

```
RFController(config-rtls-sole)#aap-rssi-update-interval 99
RFController(config-rtls-sole)#
```

wireless-client

SOLE config commands

Displays wireless-client configurations

Supported in the following platforms:

- Mobility RFS4000 Controller
- Mobility RFS6000 Controller
- Mobility RFS7000 Controller

Syntax

```
wireless-client power-level <1-100>
```

Parameters

wireless-client powerlevel <1-100>]	Displays wireless-client configurations • power-level <1-100> – Displays wireless-client power-level

Example

```
RFController(config-rtls-sole)#wireless-client powerlevel 9
RFController(config-rtls-sole)#
```

Chapter

Smart RF Instance

25

In this chapter

Use the `(config-wireless-smart-rf)` instance to configure Smart RF related configuration commands. To navigate to the `config-wireless-smart-rf` instance, use the following commands:

```
RFController(config)#wireless
RFController(config-wireless)#smart-rf
RFController(config-wireless-smart-rf)#
```

smart-rf config commands

The following table summarizes **`config-wireless-smart-rf`** commands:

TABLE 27 Smart-RF Configuration Commands

Command	*Description*	*Ref.*
assignable-power-range	Specifies the power range during power-assignment	*page 769*
auto-assign	Enables individual RF parameters to be auto-assigned	*page 770*
clrscr	Clears the display screen	*page 771*
end	Ends the current mode and moves to the PRIV EXEC mode	*page 772*
exit	Ends the current mode and moves to the previous mode	*page 773*
extensive-scan	Enables the extensive-scan mode, calibrations to be made at every tx-power level	*page 774*
help	Displays the interactive help system	*page 775*
hold-time	The number of seconds to disable interference avoidance after a detection	*page 776*
no	Negates commands or resets values to default	*page 777*
number-of-rescuers	Sets the number of rescuers to cover for faulty radios	*page 781*
radio	Smart RF radio related commands	*page 782*
recover	Enables individual self-recovery features	*page 785*
retry-threshold	Sets the average number of retries before a channel scan is performed	*page 786*
run-calibrate	Starts a new automatic RF calibration process	*page 787*
scan-dwell-time	Sets the time duration to dwell on a channel during channel scan	*page 788*

TABLE 27 Smart-RF Configuration Commands

Command	Description	Ref.
schedule-calibrate	Sets the parameters for auto-calibrate	*page 789*
select-channels	Selects channels for automatic channel scan and Smart RF	*page 790*
service	Service commands that sets Smart RF parameters	*page 791*
show	Shows the running Smart RF information	*page 794*
smart-rf-module	Enables the Smart RF module	*page 798*
verbose	Enables the verbose mode that records every Smart RF assignment	*page 799*

assignable-power-range

smart-rf config commands

Specifies the power range during power assignment.

Supported in the following platforms:

- Mobility RFS4000 Controller
- Mobility RFS6000 Controller
- Mobility RFS7000 Controller

Syntax

```
assignable-power-range [<lower bound> <upper bound>]
```

Parameters

assignable-power-range [<lower bound> <upper bound>]	Specifies the power range during power assignment. • lower bound – The lower bound of the power range. Value is between 4 and 20. • Upper bound – The upper bound of the power range. Value is between 4 and 20.

Example

```
RFController(config-wireless-smart-rf)#assignable-power-range 4 10
RFController(config-wireless-smart-rf)#
```

auto-assign

smart-rf config commands

Enables individual RF parameters to be auto-assigned

Supported in the following platforms:

- Mobility RFS4000 Controller
- Mobility RFS6000 Controller
- Mobility RFS7000 Controller

Syntax

```
auto-assign [all|channel|detector|power|rescuer] enable
```

Parameters

auto-assign [all|channel|detector|power| rescuer] enable	Enables individual RF parameters to be auto-assigned. • all - Enables auto-assign for all the RF parameters • channel enable - Enables auto-assign for channels • detector enable - Enables auto-assign for detectors • power enable - Enables auto-assign for power • rescuer enable - Enables auto-assign for rescuer

Example

```
RFSController(config-wireless-smart-rf)#auto-assign all enable
RFSController(config-wireless-smart-rf)#auto-assign channel enable
RFSController(config-wireless-smart-rf)#auto-assign detector enable
RFSController(config-wireless-smart-rf)#auto-assign power enable
RFSController(config-wireless-smart-rf)#auto-assign rescuer enable
```

clrscr

smart-rf config commands

Clears the display screen

Supported in the following platforms:

- Mobility RFS4000 Controller
- Mobility RFS6000 Controller
- Mobility RFS7000 Controller

Syntax

```
clrscr
```

Parameters

None

Example

```
RFController(config-wireless-smart-rf)#clrscr
RFController(config-wireless-smart-rf)#
```

end

smart-rf config commands

Ends and exits the current mode and moves to the PRIV EXEC mode. The prompt changes to `RFController#`

Supported in the following platforms:

- Mobility RFS4000 Controller
- Mobility RFS6000 Controller
- Mobility RFS7000 Controller

Syntax

```
end
```

Parameters

None

Example

```
RFController(config-wireless-smart-rf)#end
RFController#
```

exit

smart-rf config commands

Ends the current mode and moves to the previous mode (`config-wireless`). The prompt changes to `RFController(config-wireless)#`

Supported in the following platforms:

- Mobility RFS4000 Controller
- Mobility RFS6000 Controller
- Mobility RFS7000 Controller

Syntax

```
exit
```

Parameters

None

Example

```
RFController(config-wireless-smart-rf)#exit
RFController(config-wireless)#
```

extensive-scan

smart-rf config commands

Enters the extensive scan mode

The device needs calibration at every `tx-power` level.

Supported in the following platforms:

- Mobility RFS4000 Controller
- Mobility RFS6000 Controller
- Mobility RFS7000 Controller

Syntax

```
extensive-scan enable
```

Parameters

extensive enable	Enables the extensive scan mode.

Example

```
RFController(config-wireless-smart-rf)#extensive-scan enable
RFController(config-wireless-smart-rf)#
```

help

smart-rf config commands

Displays the system's interactive help in HTML format

Supported in the following platforms:

- Mobility RFS4000 Controller
- Mobility RFS6000 Controller
- Mobility RFS7000 Controller

Syntax

```
help
```

Parameters

None

Example

```
RFController(config-wireless-smart-rf)#help
CLI provides advanced help feature.  When you need help,
anytime at the command line please press '?'.

If nothing matches, the help list will be empty and you must backup
until entering a '?' shows the available options.
Two styles of help are provided:
1. Full help is available when you are ready to enter a
   command argument (e.g. 'show ?') and describes each possible
   argument.
2. Partial help is provided when an abbreviated argument is entered
   and you want to know what arguments match the input
   (e.g. 'show ve?'.)

RFController(config-wireless-smart-rf)#
```

hold-time

smart-rf config commands

Defines the number of seconds to disable interference avoidance after a detection

This prevents a radio from changing channels continuously.

Supported in the following platforms:

- Mobility RFS4000 Controller
- Mobility RFS6000 Controller
- Mobility RFS7000 Controller

Syntax

```
hold-time <30-65535>
```

Parameters

hold-time *<30-65535>*	The number of seconds to disable interface avoidance after a detection. This prevents the radio from changing channels continuously. Set the values in seconds from 30-65535.

Example

```
RFController(config-wireless-smart-rf)#hold-time 400
RFController(config-wireless-smart-rf)#
```

no

smart-rf config commands

Disables the Smart RF configurations

Supported in the following platforms:

- Mobility RFS4000 Controller
- Mobility RFS6000 Controller
- Mobility RFS7000 Controller

Syntax

```
no [assignable-power-range|auto-assign|extensive-scan|
hold-time|number-of-rescuers|radio|recover|
retry-threshold|scan-dwell-time|schedule-calibrate|
select-channels|service|smart-rf-module|verbose]

no assignable-power-range [<4-20> <4-20>]

no auto-assign [all|channel|detector|power|rescuer]

no extensive-scan enable

no number-of-rescuers

no radio [<1-4096>|MAC-ADDRESS|RADIO|all-11a|all-11b|
all-11bg]

no recover [coverage-hole|interference|neighbor] enable

no retry-threshold [<0.0-15.0>]
no scan-dwell-time [<1-10>]
no schedule-calibrate [enable|interval|start-time]
no select-channels <WORD>
no service smart-rf [max-history|replay enable|rescue]
no smart-rf-module enable
no verbose
```

Parameters

assignable-power-*range* *<4-20> <4-20>*	Negates the power range assignment.
auto-assign [all |channel |detector|power|rescuer] enable	Negates the auto-assign commands • all - Disables all auto-assignment features • channel enable – Disables channel assignments • detector enable – Disables detector assignments • power enable – Disables power assignments • rescuer enable – Disables rescuer assignments
extensive-scan enable	Disables the extensive scan mode
hold-time *<30-65535>*	Disables hold-time for interference avoidance. Set the value in seconds from 30-65535.
number-of-rescuers	Reverts to the default number of rescuers to cover faulty radio

radio [*<1-4096>*| *MAC- Address*|*RADIO*| all-11a|all-11b|all-11bg]	Negates all radio related commands.
	• <1-4096> – For each of the radio, the following values are negated or reset:
	  • antenna-gain <GAIN> – Resets the set antenna gain value.
	  • coverage-rate [1|2|5p5|6|9|11|12|18|24|36|48|54] – Resets the selected coverage rate value.
	  • lock-auto-assign [all | channel | detector | power | rescuer] – Resets the lock auto assign value.
	  • radio-mac [AA-BB-CC-DD-EE-FF] – Resets the selected Radio MAC address
	  • rescuer [AA-BB-CC-DD-EE-FF | all] – Resets the selected rescuer MAC address or resets all the rescuers.
	• *AA-BB-CC-DD-EE-FF* – For the selected Radio MAC, the following parameters are negated or reset.
	  • antenna-gain <GAIN> – Resets the set antenna gain value.
	  • coverage-rate [1|2|5p5|6|9|11|12|18|24|36|48|54] - Resets the selected coverage rate value.
	  • lock-auto-assign [all | channel | detector | power | rescuer] – Resets the lock auto assign value.
	• *RADIO* – A list of radio index values such as *1,3,5* or *3-7* the following parameter values are negated or reset

radio [*<1-4096>*|*MAC Address*|*RADIO*| all-11a|all-11b|all-11bg] (contd....)	• all-11a - for all 802.11a radios, the following values are negated or reset:
	  • antenna-gain <GAIN> – Resets the set antenna gain value.
	  • coverage-rate [1|2|5p5|6|9|11|12|18|24|36|48|54)]- Resets the selected coverage rate value.
	  • lock-auto-assign [all | channel | detector | power | rescuer] - Resets the lock auto assign value.
	• all-11b - for all 802.11b radios, the following values are negated or reset:
	  • antenna-gain <GAIN> – Resets the set antenna gain value.
	  • coverage-rate [1|2|5p5|6|9|11|12|18|24|36|48|54] – Resets the selected coverage rate value.
	  • lock-auto-assign [all | channel | detector | power | rescuer] – Resets the lock auto assign value.
	• all-11bg - for all 802.11bg radios, the following values are negated or reset:
	  • antenna-gain <GAIN> – Resets the set antenna gain value.
	  • coverage-rate [1|2|5p5|6|9|11|12|18|24|36|48|54] – Resets the selected coverage rate value.
	  • lock-auto-assign [all | channel | detector | power | rescuer] – Resets the lock auto assign value.

recover [coverage-hole| interference|neighbor] enable	Negates recover commands. • coverage-hole enable – Negates the command to recover from coverage-hole. • interference enable – Negates the command to recover from interference. • neighbor enable – Negates the command to recover from faulty neighbor radio condition.
retry-threshold [*<0.0-15.0>*]	Resets recovery-threshold values to default.
scan-dwell-time *<1-10>*	Resets the time a scan dwells on a channel during scan.
schedule-calibrate [enable|interval| start-time]	Resets the calibration schedule parameters. • enable – Disables the calibration schedule feature. • interval – Negates the calibration schedule interval. • start-time – Negates the calibration schedule start time.
service smart-rf [max-history|replay (enable)|rescue]	Resets the Smart RF related service commands. • smart-rf max-history – Resets the maximum number history entries. • replay enable – Disables the replay mode. • rescue <WORD> – Removes rescue operation • WORD – A single radio MAC address
select-channels <WORD>	Revert selected- channels to default • WORD– A comma-separated list of channels
smart-rf-module enable	Disables the feature
verbose enable	Disables the verbose mode of recording every assignment.

Example

```
RFController(config-wireless-smart-rf)#no ?
assignable-power-range  reset the power range to default
auto-assign             disable individual RF parameters to beauto-assigned
extensive-scan          extensive scan mode, calibrate at everytx-power level
hold-time               The number of seconds to disable
                                interference avoidance after a detection.
                                This prevents a radio from changing
                                channels continuously
number-of-rescuers      revert to default the number of rescuers to cover
faulty radio

radio                   Radio related commands
recover                 disable individual self-recovery features
retry-threshold         The average number retries to cause a radio to re-run
channel selection

scan-dwell-time         The number of seconds to dwell on a
                                channel during scan
schedule-calibrate      configure calibration schedule parameters
select-channels         Revert selected-channels to default
service                 Service Commands
smart-rf-module         smart-rf module
verbose                 verbose mode, record every assignment

RFController(config-wireless-smart-rf)#

RFController(config-wireless-smart-rf)#no assignable-power-range
RFController(config-wireless-smart-rf)#
RFController(config-wireless-smart-rf)#no auto-assign all enable
RFController(config-wireless-smart-rf)#
RFController(config-wireless-smart-rf)#no extensive-scan enable
RFController(config-wireless-smart-rf)#
RFController(config-wireless-smart-rf)#no hold-time 100
RFController(config-wireless-smart-rf)#
RFController(config-wireless-smart-rf)#no number-of-rescuers
RFController(config-wireless-smart-rf)#
RFController(config-wireless-smart-rf)#no radio 1 antenna-gain 10
RFController(config-wireless-smart-rf)#
RFController(config-wireless-smart-rf)#no radio all-11a antenna-gain 10
RFController(config-wireless-smart-rf)#
RFController(config-wireless-smart-rf)#no recover coverage-hole enable
RFController(config-wireless-smart-rf)#
RFController(config-wireless-smart-rf)#no retry-threshold 10.0
RFController(config-wireless-smart-rf)#
RFController(config-wireless-smart-rf)#no scan-dwell-time 10
RFController(config-wireless-smart-rf)#
RFController(config-wireless-smart-rf)#no schedule-calibrate enable
RFController(config-wireless-smart-rf)#
RFController(config-wireless-smart-rf)#no select-channels
RFController(config-wireless-smart-rf)#
RFController(config-wireless-smart-rf)#no service smart-rf max-history
RFController(config-wireless-smart-rf)#
RFController(config-wireless-smart-rf)#no smart-rf-module enable
RFController(config-wireless-smart-rf)#
RFController(config-wireless-smart-rf)#no verbose enable
RFController(config-wireless-smart-rf)#
```

number-of-rescuers

smart-rf config commands

Configures the number of rescuers to cover faulty radio conditions

Supported in the following platforms:

- Mobility RFS4000 Controller
- Mobility RFS6000 Controller
- Mobility RFS7000 Controller

Syntax

```
number-of-rescuers <1-5>
```

Parameters

number-of-rescuers <1-5>	The number of rescuers to use to cover faulty radio conditions.

Example

```
RFController(config-wireless-smart-rf)#number-of-rescuers 2
RFController(config-wireless-smart-rf)#
```

radio

smart-rf config commands

Configures the different Smart RF radio parameters

Supported in the following platforms:

- Mobility RFS4000 Controller
- Mobility RFS6000 Controller
- Mobility RFS7000 Controller

Syntax

```
radio [<1-4096>|MAC-ADDRESS|RADIO|all-11a|all-11b|all-11bg]

radio <1-4096> [antenna-gain|coverage-rate|
lock-auto-assign | radio-mac | rescuer | width]
radio <1-4096> anternna-gain <GAIN>
radio <1-4096> coverage-rate [1|2|5p5|6|9|11|12|18|24|36|48|54]
radio <1-4096> lock-auto-assign [all|channel|detector|power|rescuer]
radio <1-4096> radio-mac [MAC-ADDRESS]
radio <1-4096> rescuer [MAC-ADDRESS <4-20> <0-65535>]
radio <1-4096> width [auto|dual|single]

radio MAC-ADDRESS anternna-gain <GAIN>

radio MAC-ADDRESS coverage-rate [1|2|5p5|6|9|11|12|18|24|36|48|54]
radio MAC-ADDRESS lock-auto-assign [all|channel|detector|power|rescuer]

radio RADIO anternna-gain <GAIN>
radio RADIO coverage-rate [1|2|5p5|6|9|11|12|18|24|36|48|54]
radio RADIO lock-auto-assign [all|channel|detector|power|rescuer]

radio all-11a anternna-gain <GAIN>

radio all-11a coverage-rate [1|2|5p5|6|9|11|12|18|24|36|48|54]
radio all-11a lock-auto-assign [all|channel|detector|power|rescuer]

radio all-11b anternna-gain <GAIN>

radio all-11b coverage-rate [1|2|5p5|6|9|11|12|18|24|36|48|54]
radio all-11b lock-auto-assign [all|channel|detector|power|rescuer]

radio all-11bg anternna-gain <GAIN>

radio all-11bg coverage-rate [1|2|5p5|6|9|11|12|18|24|36|48|54]
radio all-11bg lock-auto-assign [all|channel|detector|power|rescuer]
```

Parameters

<*1-4096*> [antenna-gain | coverage-rate | lock-auto-assign | radio-mac | rescuer]	Sets the following parameters for the selected radio: • antenna-gain <GAIN> – Sets the antenna-gain value to GAIN for the selected radio. • coverage-rate [1|2|5p5|6|9|11|12|18|24|36|48|54] – Sets the coverage rate threshold value for under-coverage detection to the selected value from the list. • lock-auto-assign [all|channel|detector|power|rescuer] – Locks rf configuration from automatic smart rf assignments. • radio-mac <AA-BB-CC-DD-EE-FF> – Sets the radio MAC address for the radio with the selected index. • rescuer {AA-BB-CC-DD-EE-FF <*4-20*> <*0-65535*> } – Sets the MAC address for the rescuer radio. The following parameters are also set: • <*4-20*> – Boost power to cover for the defective radio. • <*0-65535*> – Attenuation from the rescuer radio to the selected radio. This is for information purposes only. • width [auto|dual|single] - Configures channel-width preference during calibration • auto - Auto channel-width - lets smart-rf figure out the best channel-width • dual - Dual channel-width - 40 MHz • single - Single channel-width - 20 MHz
AA-BB-CC-DD-EE-FF [antenna-gain | coverage-rate | lock-auto-assign | rescuer]	Sets the following parameters for the selected radio. • antenna-gain <GAIN> – Sets the antenna-gain value to GAIN for the selected radio. • coverage-rate [1|2|5p5|6|9|11|12|18|24|36|48|54] – Sets the coverage rate threshold value for under-coverage detection to the selected value from the list. • lock-auto-assign [all|channel|detector|power|rescuer] – Locks rf configuration from automatic smart rf assignments. • rescuer {AA-BB-CC-DD-EE-FF <*4-20*> <*0-65535*> }– Sets the MAC address for the rescuer radio. The following parameters are also set: • <*4-20*> – Boost power to cover for the defective radio. • <*0-65535*> – Attenuation from the rescuer radio to the selected radio. This is for information purposes only.
RADIO [antenna-gain| coverage-rate| lock-auto-assign]	Sets the radio parameters to a set of radio indices. • antenna-gain <GAIN> – Sets the antenna-gain value to GAIN for the selected radio. • coverage-rate [1|2|5p5|6|9|11|12|18|24|36|48|54] – Sets the coverage rate threshold value for under-coverage detection to the selected value from the list. • lock-auto-assign [all|channel|detector|power|rescuer] – Locks rf configuration from automatic smart rf assignments.
all-11a [antenna-gain| coverage-rate|lock-auto-assign]	Sets the radio parameters for all 802.11a radios. • antenna-gain <GAIN> – Sets the antenna-gain value to GAIN for the selected radio. • coverage-rate [1|2|5p5|6|9|11|12|18|24|36|48|54] – Sets the coverage rate threshold value for under-coverage detection to the selected value from the list. • lock-auto-assign [all|channel|detector|power|rescuer] – Locks rf configuration from automatic smart rf assignments.

all-11b [antenna-gain| coverage-rate| lock-auto-assign]	Sets the radio parameters for all 802.11b radios. • antenna-gain <GAIN> – Sets the antenna-gain value to GAIN for the selected radio. • coverage-rate [1|2|5p5|6|9|11|12|18|24|36|48|54] – Sets the coverage rate threshold value for under-coverage detection to the selected value from the list. • lock-auto-assign [all|channel|detector|power|rescuer] – Locks rf configuration from automatic smart rf assignments.
all-11bg [antenna-gain| coverage-rate| lock-auto-assign]	Sets the radio parameters for all 802.11bg radios. • antenna-gain <GAIN> – Sets the antenna-gain value to GAIN for the selected radio. • coverage-rate [1|2|5p5|6|9|11|12|18|24|36|48|54] – Sets the coverage rate threshold value for under-coverage detection to the selected value from the list. • lock-auto-assign [all|channel|detector|power|rescuer] – Locks rf configuration from automatic smart rf assignments.

Example

```
RFController(config-wireless-smart-rf)#radio 1 antenna-gain 20
RFController(config-wireless-smart-rf)#radio 1 coverage-area 18
RFController(config-wireless-smart-rf)#radio 1 lock-auto-assign channel
RFController(config-wireless-smart-rf)#radio 1 radio-mac 1-2-3-4-5-6
RFController(config-wireless-smart-rf)#radio 1 rescuer 1-2-3-4-5-6 20 30
RFController(config-wireless-smart-rf)#radio 1-2-3-4-5-6 antenna-gain 20
RFController(config-wireless-smart-rf)#radio 2-5,8,11,15 antenna-gain 20
RFController(config-wireless-smart-rf)#radio all-11a coverage-rate 5p5
RFController(config-wireless-smart-rf)#radio all-11b lock-auto-assign power
RFController(config-wireless-smart-rf)#radio all-llbg antenna-gain 20
RFController(config-wireless-smart-rf)#radio 1 width dual
RFController(config-wireless-smart-rf)#
```

recover

smart-rf config commands

Enables individual self-recovery features

Supported in the following platforms:

- Mobility RFS4000 Controller
- Mobility RFS6000 Controller
- Mobility RFS7000 Controller

Syntax

```
recover [coverage-hole|interference|neighbor]
```

Parameters

recover [coverage-hole| interference|neighbor] enable	Enables individual self recovery features: • coverage-hole enable – Enables recovery from coverage-hole errors • interference enable – Enables recovery from interference errors • neighbor enable – Enables recovery from errors due to faulty neighbor radios

Example

```
RFController(config-wireless-smart-rf)#recover coverage-hole enable
RFController(config-wireless-smart-rf)#recover interference enable
RFController(config-wireless-smart-rf)#recover neighbor enable
RFController(config-wireless-smart-rf)#
```

retry-threshold

smart-rf config commands

Sets the threshold for the average number of retries performed before a radio re-runs a channel scan

Supported in the following platforms:

- Mobility RFS4000 Controller
- Mobility RFS6000 Controller
- Mobility RFS7000 Controller

Syntax

```
retry-threshold <0.0-15.0>
```

Parameters

<0.0-15.0>	The value in decimal number. This is the average number of retries a radio makes before it re-runs the channel scan.

Example

```
RFController(config-wireless-smart-rf)#retry-threshold 8.4
RFController(config-wireless-smart-rf)#
```

run-calibrate

smart-rf config commands

Starts an automatic RF configuration process

Supported in the following platforms:

- Mobility RFS4000 Controller
- Mobility RFS6000 Controller
- Mobility RFS7000 Controller

Syntax

```
run-caliberate
```

Parameters

None

Example

```
run-caliberate
```

scan-dwell-time

smart-rf config commands

Sets the time in seconds to dwell on a channel during a channel scan

Supported in the following platforms:

- Mobility RFS4000 Controller
- Mobility RFS6000 Controller
- Mobility RFS7000 Controller

Syntax

```
scan-dwell-time <1-10>
```

Parameters

scan-dwell-time <1-10>	The duration in seconds to dwell on a channel during a channel scan. The default scan dwell time value is 1 second. If the scan dwell time is increased, the same time will be required to scan each channel which increases the total calibration time thus causing the disruption of service during that time.

Example

```
RFController(config-wireless-smart-rf)#scan-dwell-time 10
RFController(config-wireless-smart-rf)#
```

schedule-calibrate

smart-rf config commands

Configures the calibrate schedule parameters

This is used to configure parameters that schedule the automatic configuration of the Smart RF feature.

Supported in the following platforms:

- Mobility RFS4000 Controller
- Mobility RFS6000 Controller
- Mobility RFS7000 Controller

Syntax

```
schedule-calibrate [enable |interval |start-time]
schedule-calibrate interval <1-366>
    schedule-calibrate start-time <HH:MM> <1-31> <1-12>
<2008-2035>
```

Parameters

enable	Enables the schedule-calibrate feature. When enabled, the Smart RF auto calibration feature is performed at the set interval.
interval <*1-366*>	Sets the interval in days between each auto calibration.
start-time <*HH:MM*> <*1-31*> <*1-12*> <2008-2035>	Sets the time and day to start the first auto-calibration. <HH:MM> is in 24 hours format.

Example

```
RFController(config-wireless-smart-rf)#schedule-calibrate enable
RFController(config-wireless-smart-rf)#schedule-calibrate interval 2
RFController(config-wireless-smart-rf)#schedule-calibrate
                                              start-time 10:30 1 1
RFController(config-wireless-smart-rf)#
```

select-channels

smart-rf config commands

Selects a list of channels for Automatic Channel Scan and Smart RF

Use this command to add channels or remove them from the channel list.

Supported in the following platforms:

- Mobility RFS4000 Controller
- Mobility RFS6000 Controller
- Mobility RFS7000 Controller

Syntax

```
select-channel [<WORD>|add<WORD>|remove <WORD>]
```

Parameters

<WORD>	A comma separated list of channel numbers.
add <WORD>)	Add a channel or a list of channels to the channel list.
remove <WORD>	Remove a channel or a list of channels from the channel list

Example

```
RFController(config-wireless-smart-rf)#select-channels 1,2,15-17
RFController(config-wireless-smart-rf)#select-channels add 1,2,15-17
RFController(config-wireless-smart-rf)#select-channels remove 1,2,15-17
RFController(config-wireless-smart-rf)#
```

service

smart-rf config commands

Invokes service commands to troubleshoot or debug `(config-wireless-smart-rf)` instance configurations

Supported in the following platforms:

- Mobility RFS4000 Controller
- Mobility RFS6000 Controller
- Mobility RFS7000 Controller

Syntax

```
service show cli
service smart-rf [clear-history|load-from-file|max-history
|replay|rescue|restore|save-to-file|simulate|step-calibrate]

service smart-rf clear-history
service smart-rf load-from-file
service smart-rf max-history <0-65535>
service smart-rf replay enable
service smart-rf rescue <WORD>
service smart-rf restore [WORD]
service smart-rf save-to-file
service smart-rf simulate [coverage-hole <1-4096> UINT_RANGE
{UINT_RANGE|pattern-11a|pattern-11b|
pattern-11bg|pattern-2-mbps}|interference]

service smart-rf simulate interference <WORD>

service smart-rf step-calibrate [assign-channel|
assign-detectors|assign-power|assign-prepare|
assign-rescuers|collect-data|prepare-detectors|
pull-rf-config|push-rf-config|sync-rf-config]
```

Parameters

show cli	Displays the CLI tree of the current mode.

smart-rf [clear-history | load-from-file | max-history | replay | rescue | restore | save-to-file | simulate | step-calibrate]	Smart RF related commands are executed from this service command.
	• clear-history – Clears assignment history
	• load-from-file – Loads Smart RF record from file *smart.bin*
	• max-history <*0-65535*> – Sets the number of assignment items to be retained as history.
	• replay enable – Enables the Smart RF replay mode
	• rescue <WORD> – Enables force rescue operation
	• restore <WORD> – Removes any recovering operation on given radio
	• save-to-file – Saves Smart RF records to the local file *smart.bin*
	• simulate [coverage-hole | interference] – Simulates the different radio events
	  • coverage-hole <UINT_RANGE> – Simulates the coverage-hole event
	  • UINT_RANGE [pattern-11a | pattern-11b | pattern11bg | pattern-2-mbps] – provide simulated Client's allowed
	  • interference – Simulates radio interferences
	• step-calibrate [assign-channels | assign-detectors | assign-power | assign-prepare | assign-rescuers | collect-data | prepare-detectors | pull-rf-config | push-rf-config | sync-rf-config] – Manages Smart-RF commands
	  • assign-channels – Assigns channels to radios
	  • assign-detectors – Assigns detectors
	  • assign-power – Assigns tx power to radios

	• assign-prepare – Prepares assignment • assign-rescuers – Assigns rescuers along with recovering power • collect-data – Collects site measurement data • prepare-detectors – Prepare prior to assign detectors • pull-rf-config – Pull RF-configuration from cluster members • push-rf-config – Push Rf-configuration to cluster members • sync-rf-config – Sync RF-configuration of cluster members

Example

```
RFController(config-wireless-smart-rf)#service show cli
Smart-RF Configuration mode:
+-assignable-power-range
  +-<4-20>
    +-<4-20> [assignable-power-range <4-20> <4-20>]
+-auto-assign
  +-all
    +-enable [auto-assign (detector|channel|power|rescuer|all) enable]
  +-channel
    +-enable [auto-assign (detector|channel|power|rescuer|all) enable]
  +-detector
```

```
    +-enable [auto-assign (detector|channel|power|rescuer|all) enable]
  +-power
    +-enable [auto-assign (detector|channel|power|rescuer|all) enable]
  +-rescuer
    +-enable [auto-assign (detector|channel|power|rescuer|all) enable]
+-clrscr [clrscr]
+-end [end]
+-exit [exit]
+-extensive-scan
  +-enable [(smart-rf-module|verbose|extensive-scan) enable]
+-help [help]
+-hold-time
  +-<30-65535> [hold-time <30-65535>]
+-no
  +-assignable-power-range [no assignable-power-range]
  +-auto-assign
    +-all
      +-enable [no auto-assign (detector|channel|power|rescuer|all) enable]
    +-channel
      +-enable [no auto-assign (detector|channel|power|rescuer|all) enable]
    +-detector
      +-enable [no auto-assign (detector|channel|power|rescuer|all) enable]
    +-power
      +-enable [no auto-assign (detector|channel|power|rescuer|all) enable]
    +-rescuer
      +-enable [no auto-assign (detector|channel|power|rescuer|all) enable]
  +-extensive-scan
    +-enable [no (smart-rf-module|verbose|extensive-scan) enable]
  +-hold-time [no hold-time (|<30-65535>)]
    +-<30-65535> [no hold-time (|<30-65535>)]
  +-number-of-rescuers [no number-of-rescuers]


.....


+-smart-rf-module
  +-enable [(smart-rf-module|verbose|extensive-scan) enable]
+-verbose
  +-enable [(smart-rf-module|verbose|extensive-scan) enable]
+-write
  +-memory [write memory]
```

show

smart-rf config commands

Displays current system information

Supported in the following platforms:

- Mobility RFS4000 Controller
- Mobility RFS6000 Controller
- Mobility RFS7000 Controller

NOTE
The following commands display only for the Mobility RFS6000 Controller and the Mobility RFS4000 Controller
- power
The following commands display only for the Mobility RFS7000 Controller and the Mobility RFS4000 Controller:
- port-channel
- static-channel-group

Syntax

```
show <parameters>
show wireless smart-rf [calibration-status|configuration| history |radio]
show wireless smart-rf calibration-status
show wireless smart-rf configuration
show wireless smart-rf history

show wireless smart-rf radio [config|local-status|map|
master-status|neighbors|spectrum]

show wireless smart-rf radio config[<1-4096>|MAC_ADDRESS
|all-11a|all-11bg]

show wireless smart-rf radio local-status[<1-4096>|
MAC_ADDRESS|all-11a|all-11bg]

show wireless smart-rf radio map [MAC_ADDRESS|all-11a|
all-11bg]
show wireless smart-rf radio master-status [MAC_ADDRESS|
all-11a|all-11bg]
show wireless smart-rf radio neighbors [MAC_ADDRESS|
all-11a|all-11bg]
show wireless smart-rf radio spectrum [MAC_ADDRESS|
all-11a|all-11bg]
```

Parameters

?	Displays the parameters for which information can be viewed using the show command

Example

```
RFController(config-wireless-smart-rf)#show ?
  access-list           Internet Protocol (IP)
  aclstats              Show ACL Statistics information
  alarm-log             Display all alarms currently in the system
```

```
  autoinstall           autoinstall configuration
  banner                Display Message of the Day Login banner
  boot                  Display boot configuration.
  clock                 Display system clock
  commands              Show command lists
  crypto                encryption module
  debugging             Debugging information outputs
  dhcp                  DHCP Server Configuration
  environment           show environmental information
  file                  Display filesystem information
  firewall              Wireless firewall
  ftp                   Display FTP Server configuration
  history               Display the session command history
  interfaces            Interface status
  ip                    Internet Protocol (IP)
  ldap                  LDAP server
  licenses              Show any installed licenses
  logging               Show logging configuration and buffer
  mac                   Internet Protocol (IP)
  mac-address-table     Display MAC address table
  management            Display L3 Managment Interface name
  mobility              Display Mobility parameters
  ntp                   Network time protocol
  password-encryption   password encryption
  port                  Physical/Aggregate port interface
  port-channel          Portchannel commands
  privilege             Show current privilege level
  protocol-list         List of protocols
  radius                RADIUS configuration commands
  role                  Configure role parameters
  redundancy            Display redundancy group parameters
  rtls                  Real Time Locating System commands
  running-config        Current Operating configuration
  securitymgr           Securitymgr parameters
  sessions              Display current active open connections
  service-list          List of services
  snmp                  Display SNMP engine parameters
  snmp-server           Display SNMP engine parameters
  spanning-tree         Display spanning tree information
  startup-config        Contents of startup configuration
  static-channel-group  static channel group membership
  terminal              Display terminal configuration parameters
  timezone              Display timezone
  traffic-shape         Display traffic shaping
  upgrade-status        Display last image upgrade status
  users                 Display information about currently logged
                        in users
  version               Display software & hardware version
  virtual-ip            IP redundancy feature
  wireless              Wireless configuration commands
  wlan-acl              wlan based acl

RFController(config-wireless-smart-rf)#show wireless ? aap-version
The minimum Adaptive firmware version string
  ap                          Status of adopted access-point
  ap-containment              Rogue AP Containment
  ap-detection-config         Detected-AP Configuration Parameters
  ap-images                   List of access-point images on the
                                    wireless controller
  ap-unadopted                List of unadopted access-point
```

```
  approved-aps                Approved APs seen by access-point
                                    scans
  channel-power               List of available channel and power
                                    levels for a radio
  client                      wireless client configuration
  config                      Wireless Configuration Parameters
  country-code-list           List of supported country names and 2
                                    letter IS0 3166 codes
  default-ap                  Information for default access-point
  hotspot-config              Wlan hotspot configuration
  ids                         Intrusion detection parameters
  known                       Known AP related parameters
  mac-auth-local              list out the mac-auth-local entries
  mesh                        Mesh related parameters
  wireless-client                 Details of associated wireless-clients
  multicast-packet-limit      multicast-packet-limit
  phrase-to-key               display the WEP keys generated by a
                                    passphrase
  qos-mapping                 Quality of Service mappings used for
                                    mapping wireless priorities and
                                    802.1p / DSCP tags
  radio                       Radio related commands
  radio-group                 radio group configuration
  regulatory                  Regulatory (allowed channel/power)
                                    information for a particular country
  self-heal-config            Self-Healing Configuration Parameters
  sensor                      Wireless Intrusion Protection System
                                    parameters. Use "sensor vlan x" to
                                    specify the vlan(s) to which the
                                    sensors are connected.
  smart-rf                    Smart-RF Management Commands
  unapproved-aps              Unapproved APs seen by access-point or
                                    wireless-client scans
  wireless-controller-statistics  wireless-controller  statistics
  wlan                        Wireless LAN related parameters

RFController(config-wireless-smart-rf)#show wireless smart-rf ?
  calibration-status  display smart-rf calibration status
  configuration       display smart-rf configuration
  history             display smart-rf assignment history since
                            latest calibration
  radio               Radio related commands
RFController(config-wireless-smart-rf)#
```

```
RFController(config-wireless-smart-rf)#show wireless smart-rf configuration
Smart-RF Module          : disabled

Smart-RF Calibration configuration:
  auto-assign detector   : enabled
  auto-assign channel    : disabled
  auto-assign power      : enabled
  auto-assign rescuer    : enabled
  channels selected      :
  channels excluded      :
  assignable-power-range : [ 4 - 16 ] dBm
  number of rescuers     : 3
  scan dwell time        : 1 second
```

```
  retry-threshold        : 14.0 averaged retries/packet
  hold-time              : 3600 seconds

Smart-RF Calibration Schedule:
  schedule calibration   : disabled
  schedule first-start   : Sat Mar 29 03:30:00 2008
  schedule interval      : 1 day(s)

Smart-RF Run Time Monitor and Recovery configuration:
  recover interference   : enabled
  recover neighbor       : enabled
  recover coverage-hole  : enabled

Diagnostic configuration:
  Verbose Mode           : disabled
  Extensive Scan Mode    : disabled

RFController(config-wireless-smart-rf)#

RFController(config-wireless-smart-rf)#show wireless smart-rf
calibration-status

Smart-RF Calibration is busy at delay-second

Smart Master IP:     0.0.0.0
My           IP:     0.0.0.0
Cluster Master :     yes

Last Calibration Started at: Sun Sep  7 06:01:48 2008
Last Calibration Ended at:   Sun Sep  7 06:01:48 2008
Next calibration Starts at:  not scheduled

RFController(config-wireless-smart-rf)#

RFController(config-wireless-smart-rf)#show wireless smart-rf history

Smart Master IP:     0.0.0.0
My           IP:     0.0.0.0
Cluster Master :     yes

Last Calibration Started at: Sun Sep  7 06:03:33 2008
Last Calibration Ended at:   Sun Sep  7 06:03:33 2008
Next calibration Starts at:  not scheduled

Smart RF assignment history since last calibration, up to 9216 entries

RFController(config-wireless-smart-rf)#
```

smart-rf-module

smart-rf config commands

Enables the Smart RF feature

Supported in the following platforms:

- Mobility RFS4000 Controller
- Mobility RFS6000 Controller
- Mobility RFS7000 Controller

Syntax

```
smart-rf-module enable
```

Parameters

smart-rf-module enable	Enables Smart RF.

Example

```
RFController(config-wireless-smart-rf)#smart-rf-module enable
RFController(config-wireless-smart-rf)#
```

verbose

smart-rf config commands

Enables the verbose mode that records every Smart RF assignment

Supported in the following platforms:

- Mobility RFS4000 Controller
- Mobility RFS6000 Controller
- Mobility RFS7000 Controller

Syntax

```
verbose enable
```

Parameters

verbose enable	Enables the verbose mode where every Smart RF assignment is recorded.

Example

```
RFController(config-wireless-smart-rf)#verbose enable
RFController(config-wireless-smart-rf)#
```

Chapter

26

Role Instance

In this chapter

Use the `(config-role)` instance to configure Role related configuration commands. To navigate to the `config-role` instance, use the following commands:

```
RFController(config)#role <rolename> <rolepriority>
RFController(config-role)#
```

For more information on the `role` command, see *role on page 278*.

Role config commands

The following table summarizes **`config-role`** commands:

TABLE 28 Role Config Commands

Command	Description	mRef.
ap-location	Sets the AP location configuration	*page 802*
authentication -type	Sets the authentication type configuration	*page 803*
encryption-type	Sets the encryption type	*page 804*
essid	Sets ESSID configuration for role based firewall	*page 805*
group	Sets role group properties	*page 806*
ip	Sets IP configuration properties	*page 807*
mac	Sets MAC configuration properties	*page 808*
client-mac	Sets Client MAC configuration properties	*page 809*
no	Negates role commands.	*page 811*
service	Invokes service commands to troubleshoot or debug `(config-dhcp)` instance configurations	*page 815*
show	Displays the running system information	*page 816*
clrscr	Clears the display screen	*page 810*
exit	Ends the current mode and moves to the previous mode	*page 813*
end	Ends the current mode and moves to the EXEC mode	*page 812*
help	Displays the interactive help system in HTML format	*page 814*

ap-location

Role config commands

Sets the AP location configuration

- This requires the location engine to be enabled on the controller with a site, appropriate zones defined and AP co-ordinates defined. The role based firewall has to know which zone the Client is located when it associates for the ap-parameter option to work.
- The ‘ap-location’ parameter defines the zone or zones you wish to match.

Supported in the following platforms:

- Mobility RFS4000 Controller
- Mobility RFS6000 Controller
- Mobility RFS7000 Controller

Syntax

```
ap-location [any|contains|exact|not-contains]
ap-location any
ap-location contains <WORD>
ap-location exact <WORD>
ap_location not-contains <WORD>
```

Parameters

any	Defines any AP location.
contains <WORD>	AP location contains the string <WORD>.
exact <WORD>	AP location contains the exact string <WORD>
not-contains <word>	AP location does not contain the string <WORD>

Example

```
RFController(config-role)#ap-location any
RFController(config-role)#

RFController(config-role)#ap-location contains office
RFController(config-role)#


RFController(config-role)#ap-location exact warehouse
RFController(config-role)#

RFController(config-role)#ap-location not-contains office
RFController(config-role)#
```

authentication-type

Role config commands

Selects authentication type for the role

Supported in the following platforms:

- Mobility RFS4000 Controller
- Mobility RFS6000 Controller
- Mobility RFS7000 Controller

Syntax

```
authentication-type [any|eq|neq]

authentication-type any

authentication-type eq [eap|hotspot|kerberos|mac-auth|none]

authentication-type neq[eap|hotspot|kerberos|mac-auth|none]
```

Parameters

any	Any type of authentication.
eq [eap|hotspot|kerberos|mac-auth|none]	Authentication type equals one of the following: • eap – Extensible Authentication Protocol • hotspot – Hotspot authentication • kerberos – Kerberos authentication • mac-auth – MAC authentication protocol • none – no authentication used
neq [eap|hotspot|kerberos|mac-auth|none]	Authentication protocol does not contain one of the listed options.

Example

```
RFController(config-role)#authentication-type any
RFController(config-role)#
```

encryption-type

Role config commands

Selects encryption for the role

Supported in the following platforms:

- Mobility RFS4000 Controller
- Mobility RFS6000 Controller
- Mobility RFS7000 Controller

Syntax

```
encryption-type [any|eq|neq]

encryption-type any

encryption-type eq [ccmp|keyguard|none|tkip|tkip-ccmp|
wep128|wep128-keyguard|wep64]

encryption-type neq [ccmp|keyguard|none|tkip|tkip-ccmp|
wep128|wep128-keyguard|wep64]
```

Parameters

any	Encryption type can be any
eq [ccmp|keyguard|none|tkip |tkip-ccmp| wep128|wep128-keyguard |wep64]	Encryption type equals one of the following: • ccmp • keyguard • none • tkip • tkip-ccmp • wep128 • wep128-keyguard • wep64
neq [ccmp|keyguard|none|tkip |tkip-ccmp| wep128|wep128-keyguard |wep64]	Encryption type must not be one of the listed options.

Example

```
RFController(config-role)#encryption-type wep128
RFController(config-role)#
```

essid

Role config commands

Sets ESSID configuration for the role

Supported in the following platforms:

- Mobility RFS4000 Controller
- Mobility RFS6000 Controller
- Mobility RFS7000 Controller

Syntax

```
essid [any|contains|exact|not-contains]

essid any
essid contains <WORD>
essid exact <WORD>
essid not-contains <WORD>
```

Parameters

any	Any ESSID.
contains <WORD>	ESSID contains the string <WORD>.
exact <WORD>	ESSID contains the exact string <WORD>
not-contains <word>	ESSID does not contain the string <WORD>

Example

```
RFController(config-role)#essid any
RFController(config-role)#
```

group

Role config commands

Sets group configuration for the role

Supported in the following platforms:

- Mobility RFS4000 Controller
- Mobility RFS6000 Controller
- Mobility RFS7000 Controller

Syntax

```
group [any|contains|exact|not-contains]
group any
group contains <WORD>
group exact <WORD>
group not-contains <WORD>
```

Parameters

any	Any group.
contains <WORD>	Group contains the string <WORD>.
exact <WORD>	Group contains the exact string <WORD>
not-contains <word>	Group does not contain the string <WORD>

Example

```
RFController(config-role)#group any
RFController(config-role)#
```

ip

Role config commands

Sets IP parameters for the role

Supported in the following platforms:

- Mobility RFS4000 Controller
- Mobility RFS6000 Controller
- Mobility RFS7000 Controller

Syntax

```
ip access-group [<1-99>|<100-199>|<1300-1999>|
<2000-2699>|<WORD>] [in|out] acl-precedence <1-100>
```

Parameters

access-group [<1-99>| <100-199>|<1300-1999> | <2000-2699>|<WORD>] [in|out] acl-precedence <1-100>	Sets the ACL precedence for the following ACL List entries • <1-99> – IP standard access list • <100-199> – IP extended access list • <1300-1999> – IP standard access list (expanded range) • <2000-2699> – IP extended access list (expanded range) • <word> – IP access list name • in – Apply grouping to incoming packets • out – Apply grouping to outgoing packets • acl-precedence <1-100> – Sets ACL precedence to a value between 1 and 100.

Example

```
RFController(config-role)#ip access-group 8 in acl-precedence
RFController(config-role)#
```

mac

Role config commands

Sets MAC access group configuration commands

Supported in the following platforms:

- Mobility RFS4000 Controller
- Mobility RFS6000 Controller
- Mobility RFS7000 Controller

Syntax

```
mac access-group <WORD> [in|out] acl-precedence <1-100>
```

Parameters

access-group <word> [in|out] acl-precedence <1-100>	Sets MAC access group configuration parameters • <WORD> – The ACL name • in – Apply grouping to incoming packets • out – Apply grouping to outgoing packets • acl-precedence <1-100> – sets ACL precedence to a value between 1 and 100.

Example

```
RFController(config-role)#mac access-group 8 in acl-precedence
RFController(config-role)#
```

client-mac

Role config commands

Configures the Client MAC addresses for role based firewall

Supported in the following platforms:

- Mobility RFS4000 Controller
- Mobility RFS6000 Controller
- Mobility RFS7000 Controller

Syntax

```
client-mac [<MAC Address>|<MAC Address>/<Mask>|any]
```

Parameters

<MAC Address>	The address of the Client that is allowed. MAC address can be in the format AA:BB:CC:DD:EE:FF or AA-BB-CC-DD-EE-FF or AABB.CCDD.EEFF.
<MAC Address>/<Mask>	The address and mask combination for the Client to be allowed. <MAC Address> and <Mask> should be in the format AA:BB:CC:DD:EE:FF or AA-BB-CC-DD-EE-FF or AABB.CCDD.EEFF
any	Match with any MAC address.

Example

```
RFController(config-role)#client-mac aa:bb:cc:dd:ee:ff
RFController(config-role)#
```

clrscr

Role config commands

Clears the display screen

Supported in the following platforms:

- Mobility RFS4000 Controller
- Mobility RFS6000 Controller
- Mobility RFS7000 Controller

Syntax

```
clrscr
```

Parameters

None

Example

```
RFController(config-role)#clrscr
RFController(config-role)#
```

no

Role config commands

Negates role commands

Supported in the following platforms:

- Mobility RFS4000 Controller
- Mobility RFS6000 Controller
- Mobility RFS7000 Controller

Syntax

```
no [ap-location|authentication-type|encryption-type|essid|
group|ip|mac|client-mac]

no ap-location
no authentication-type
no encryption-type
no essid
no group
no ip access-group [<1-99>|<100-199>|<1300-1999>|
<2000-2699>|<WORD>] [in|out] acl-precedence <1-100>
no mac <WORD> [in|out] acl-precedence <1-100>
no client-mac
```

end

Role config commands

Exits the current mode and moves to the PRIV EXEC mode. The prompt changes to `RFController#`

Supported in the following platforms:

- Mobility RFS4000 Controller
- Mobility RFS6000 Controller
- Mobility RFS7000 Controller

Syntax

```
end
```

Parameters

None

Example

```
RFController(config-role)#end
RFController#
```

exit

Role config commands

Ends the current mode and moves to the previous mode (GLOBAL-CONFIG). The prompt changes to `RFController#(config)#`

Supported in the following platforms:

- Mobility RFS4000 Controller
- Mobility RFS6000 Controller
- Mobility RFS7000 Controller

Syntax

```
exit
```

Parameters

None

Example

```
RFController(config-role)#exit
RFController(config)#
```

help

Role config commands

Displays the system's interactive help in HTML format

Supported in the following platforms:

- Mobility RFS4000 Controller
- Mobility RFS6000 Controller
- Mobility RFS7000 Controller

Syntax

```
help
```

Parameters

None

Example

```
RFController(config-role)#help
CLI provides advanced help feature.  When you need help,
anytime at the command line please press '?'.

If nothing matches, the help list will be empty and you must backup
until entering a '?' shows the available options.
Two styles of help are provided:
1. Full help is available when you are ready to enter a
   command argument (e.g. 'show ?') and describes each possible
   argument.
2. Partial help is provided when an abbreviated argument is entered
   and you want to know what arguments match the input
   (e.g. 'show ve?'.)

RFController(config-dhcp)#
```

service

Role config commands

Invokes service commands to troubleshoot or debug `(config-role)` instance configurations

Supported in the following platforms:

- Mobility RFS4000 Controller
- Mobility RFS6000 Controller
- Mobility RFS7000 Controller

Syntax

```
service show cli
```

Parameters

None

Example

```
RFController(config-role#service show cli
DHCP Server Config mode:
+-address
  +-range
    +-A.B.C.D [address range A.B.C.D ( A.B.C.D |)]
      +-A.B.C.D [address range A.B.C.D ( A.B.C.D |)]
+-bootfile
  +-WORD [bootfile WORD]
+-class
  +-WORD [class WORD]
+-client-identifier
  +-WORD [client-identifier WORD]
+-client-name
  +-WORD [client-name WORD]
+-clrscr [clrscr]
+-ddns
 +-domainname
    +-WORD [ddns domainname WORD]
  +-multiple-user-class [ddns multiple-user-class]
  +-server
    +-A.B.C.D [ddns server A.B.C.D (A.B.C.D|)]
.......................
.....................................................
RFController(config-dhcp)#
```

show

Role config commands

Displays current system information

Supported in the following platforms:

- Mobility RFS4000 Controller
- Mobility RFS6000 Controller
- Mobility RFS7000 Controller

Syntax

```
show <paramater>
```

Parameters

?	Displays parameters for which information can be viewed using the show command

Example

```
RFController(config-role)#show ?
  access-list           Internet Protocol (IP)
  aclstats              Show ACL Statistics information
  alarm-log             Display all alarms currently in the system
  autoinstall           autoinstall configuration
  banner                Display Message of the Day Login banner
  boot                  Display boot configuration.
  clock                 Display system clock
  commands              Show command lists
  crypto                encryption module
  debugging             Debugging information outputs
  dhcp                  DHCP Server Configuration
  environment           show environmental information
  file                  Display filesystem information
  firewall              Wireless firewall
  ftp                   Display FTP Server configuration
  history               Display the session command history
  interfaces            Interface status
  ip                    Internet Protocol (IP)
  ldap                  LDAP server
  licenses              Show any installed licenses
  logging               Show logging configuration and buffer
  mac                   Internet Protocol (IP)
  mac-address-table     Display MAC address table
  management            Display L3 Managment Interface name
  mobility              Display Mobility parameters
  ntp                   Network time protocol
  password-encryption   password encryption
  port                  Physical/Aggregate port interface
  port-channel          Portchannel commands
  privilege             Show current privilege level
  protocol-list         List of protocols
  radius                RADIUS configuration commands
  role                  Configure role parameters
  redundancy            Display redundancy group parameters
  rtls                  Real Time Locating System commands
  running-config        Current Operating configuration
```

```
  securitymgr           Securitymgr parameters
  sessions              Display current active open connections
  service-list          List of services
  snmp                  Display SNMP engine parameters
  snmp-server           Display SNMP engine parameters
  spanning-tree         Display spanning tree information
  startup-config        Contents of startup configuration
  static-channel-group  static channel group membership
  terminal              Display terminal configuration parameters
  timezone              Display timezone
  traffic-shape         Display traffic shaping
  upgrade-status        Display last image upgrade status
  users                 Display information about currently logged
                        in users
  version               Display software & hardware version
  virtual-ip            IP redundancy feature
  wireless              Wireless configuration commands
  wlan-acl              wlan based acl

RFController(config-role)#
```

Chapter

AAP IP Filtering

27

In this chapter

The AAP IP Filter list mechanism (config-aap-ipfilter) creates filters based on the request received from the controller. It then applies those filters to the specified WLAN/LAN. To navigate to this instance, use the command:

```
RFController(config)#aap-ipfilter-list <filtername>
RFController(config-aap-ipfilter)#
```

AAP IP Filter config commands

Table 29 summarizes the controller **`config-aap-ipfilter`** commands

TABLE 29 AAP IP Filter Configuration Commands

Command	Description	Ref.
clear-all-rules	Clears all the configured rules	*page 820*
clrscr	Clears the display screen	*page 821*
deny	Specifies the packet to reject	*page 822*
end	Ends the current mode	*page 825*
exit	Ends the current mode and moves to the previous mode	*page 826*
help	Displays the interactive help system	*page 827*
no	Negates a command or sets its defaults	*page 828*
permit	Specifies packets to forward	*page 829*
service	Invokes the service commands to troubleshoot or debug instance configurations	*page 832*
show	Displays running system information	*page 834*

clear-all-rules

AAP IP Filter config commands

Clears all configured rules

Supported in the following platforms:

- Mobility RFS4000 Controller
- Mobility RFS6000 Controller
- Mobility RFS7000 Controller

Syntax

```
clear-all-rules
```

Parameters

None

Example

```
RFController(config-crypto-group)#clear-all-rules
RFController(config-crypto-group)#
```

clrscr

AAP IP Filter config commands

Clears the display screen

Supported in the following platforms:

- Mobility RFS4000 Controller
- Mobility RFS6000 Controller
- Mobility RFS7000 Controller

Syntax

```
clrscr
```

Parameters

None

Example

```
RFController(config-crypto-group)#clrscr
RFController(config-crypto-group)#
```

deny

AAP IP Filter config commands

Specifies packets to reject

Supported in the following platforms:

- Mobility RFS4000 Controller
- Mobility RFS6000 Controller
- Mobility RFS7000 Controller

Syntax

```
deny [all|icmp|tcp|upd|protocol]

deny [all|icmp|tcp|udp] [any|src-start-ip <IP> src-end-ip <IP>]
     [any|dst-start-ip <IP> dst-end-ip <IP>]
     [all|dst-start-port <1-65535> dst-end-port <1-65535>] rule <1-20>

deny protocol <1-254> [any|src-start-ip <IP> src-end-ip <IP>]
     [any|dst-start-ip <IP> dst-end-ip <IP>]
     [all|dst-start-port <1-65535> dst-end-port <1-65535>] rule <1-20>
```

Parameters

deny [all|icmp|tcp|udp] [any|src-start-ip <IP> srcend-ip <IP>] [any|dst-startip <IP> dst-end-ip <IP>] [all|dst-start-port <1-65535> dst-end-port <1-65535>] rule <1-20>	Use with a deny command to reject IP packets
	• deny all - Denies all the protocols
	• deny icmp - Specifies ICMP as the protocol
	• deny [tcp|udp] - Specifies TCP or UDP as the protocol
	The following parameters are common to all the protocols:
	• [any|src-start-ip <IP> src-end-ip <IP>] - any is an abbreviation for a source IP of 0.0.0.0 and end IP 255.255.255.255.
	  • src-start-ip <IP> - The keyword <src-start-ip> is the source IP address of the network. For example, 10.1.1.10/24 indicates the first 24 bits of the source IP is used for matching
	  • src-end-ip <IP> - The keyword <src-end-ip> is the source end IP address of the network.
	• [any|dst-start-ip <IP> dst-end-ip <IP>] - any is an abbreviation for a destination start / end IP of the network.
	  • dst-start-ip <IP> - Defines the destination start IP address
	  • dst-end-ip <IP> - Defines the destination end IP address
	• [all|dst-start-port <1-65535> dst-end-port <1-65535>] - Rejects all the packets.
	  • dst-start-port <1-65535> - Defines the destination start port
	  • dst-end-port <1-65535> - Defines the destination end port
	• rule <1-20> - Define an integer value between 1 and 20. This value sets the rule precedence on the AAP.

deny protocol <1-254> [any|src-start-ip <IP> srcend-ip <IP>] [any|dst-startip <IP> dst-end-ip <IP>] [all|dst-start-port <1-65535> dst-end-port <1-65535>] rule <1-20>	Denies protocols between 1 and 254.
	• [any|src-start-ip <IP> src-end-ip <IP>]- any is an abbreviation for a source IP of 0.0.0.0 and end IP 255.255.255.255
	  • src-start-ip <IP> - The keyword <src-start-ip> is the source IP address of the network. For example, 10.1.1.10/24 indicates the first 24 bits of the source IP is used for matching
	  • src-end-ip <IP> - The keyword <src-end-ip> is the source end IP address of the network
	• [any|dst-start-ip <IP> dst-end-ip <IP>] - any is an abbreviation for a destination start / end IP of the network.
	  • dst-start-ip <IP> - Defines the destination start IP address
	  • dst-end-ip <IP> - Defines the destination end IP address
	• [all|dst-start-port <1-65535> dst-end-port <1-65535>] - Rejects all the packets
	  • dst-start-port <1-65535> - Defines the destination start port
	  • dst-end-port <1-65535> - Defines the destination end port
	• rule <1-20> - Define an integer value between 1 and 20. This value sets the rule precedence on the AAP

Example

```
RFSController(config-aap-ipfilter)#deny all any dst-start-ip 172.16.10.9
dst-end-ip 172.16.10.11 dst-start-port 99 dst-end-port 100
RFSController(config-aap-ipfilter)#permit tcp src-start-ip 192.168.1.234
src-end-ip 192.168.1.9 dst-start-ip 10.0.0.0 dst-end-ip 10.0.0.255 all rule
rule 1
RFSController(config-aap-ipfilter)#
```

end

AAP IP Filter config commands

Ends and exits the current mode and changes to the PRIV EXEC mode. The prompt changes to `RFController#`

Supported in the following platforms:

- Mobility RFS4000 Controller
- Mobility RFS6000 Controller
- Mobility RFS7000 Controller

Syntax

```
end
```

Parameters

None

Example

```
RFController(config-app-ipfilter)#end
RFController#
```

exit

AAP IP Filter config commands

Ends the current mode and moves to the previous mode (GLOBAL-CONFIG). The prompt changes to `RFController(config)#`

Supported in the following platforms:

- Mobility RFS4000 Controller
- Mobility RFS6000 Controller
- Mobility RFS7000 Controller

Syntax

```
exit
```

Parameters

None

Example

```
RFController(config-aap-ipfilter)#exit
RFController(config)#
```

help

AAP IP Filter config commands

Displays the system's interactive help system

Supported in the following platforms:

- Mobility RFS4000 Controller
- Mobility RFS6000 Controller
- Mobility RFS7000 Controller

Syntax

```
help
```

Parameters

None

Example

```
RFController(config-aap-ipfilter)#help
CLI provides advanced help feature.  When you need help,
anytime at the command line please press '?'.

If nothing matches, the help list will be empty and you must backup
until entering a '?' shows the available options.
Two styles of help are provided:
1. Full help is available when you are ready to enter a
   command argument (e.g. 'show ?') and describes each possible
   argument.
2. Partial help is provided when an abbreviated argument is entered
   and you want to know what arguments match the input
   (e.g. 'show ve?'.)

RFController(config-aap-ipfilter)#
```

no

AAP IP Filter config commands

Negates a command or sets its defaults

Supported in the following platforms:

- Mobility RFS4000 Controller
- Mobility RFS6000 Controller
- Mobility RFS7000 Controller

Syntax

```
no rule <1-20>
```

Parameters

rule <1-20>	Specifies the rule to reject

Example

```
RFController(config-aap-ipfilter)#no rule 10
+-clrscr [clrscr]
```

permit

AAP IP Filter config commands

Specifies packets to permit

Supported in the following platforms:

- Mobility RFS4000 Controller
- Mobility RFS6000 Controller
- Mobility RFS7000 Controller

Syntax

```
permit [all|icmp|tcp|upd|protocol]

permit [all|icmp|tcp|udp] [any|src-start-ip <IP> src-end-ip <IP>]
        [any|dst-start-ip <IP> dst-end-ip <IP>]
        [all|dst-start-port <1-65535> dst-end-port <1-65535>] rule <1-20>

permit protocol <1-254> [any|src-start-ip <IP> src-end-ip <IP>]
       [any|dst-start-ip <IP> dst-end-ip <IP>]
       [all|dst-start-port <1-65535> dst-end-port <1-65535>] rule <1-20>
```

Parameters

permit [all|icmp|tcp|udp] [any|src-start-ip <IP> srcend-ip <IP>] [any|dst-startip <IP> dst-end-ip <IP>] [all|dst-start-port <1-65535> dst-end-port <1-65535>] rule <1-20>	Use with a permit command to allow IP packets
	• permit all - Permits all the protocols
	• permit icmp - Specifies ICMP as the protocol
	• permit [tcp|udp] - Specifies TCP or UDP as the protocol
	The following parameters are common to all the protocols:
	• [any|src-start-ip <IP> src-end-ip <IP>] - any is an abbreviation for a source IP of 0.0.0.0 and end IP 255.255.255.255.
	  • src-start-ip <IP> - The keyword <src-start-ip> is the source IP address of the network. For example, 10.1.1.10/24 indicates the first 24 bits of the source IP is used for matching
	  • src-end-ip <IP> - The keyword <src-end-ip> is the source end IP address of the network.
	• [any|dst-start-ip <IP> dst-end-ip <IP>] - any is an abbreviation for a destination start / end IP of the network.
	  • dst-start-ip <IP> - Defines the destination start IP address
	  • dst-end-ip <IP> - Defines the destination end IP address
	• [all|dst-start-port <1-65535> dst-end-port <1-65535>] - Accepts all the packets.
	  • dst-start-port <1-65535> - Defines the destination start port
	  • dst-end-port <1-65535> - Defines the destination end port
	• rule <1-20> - Define an integer value between 1 and 20. This value sets the rule precedence on the AAP.

permit protocol <1-254> [any|src-start-ip <IP> srcend-ip <IP>] [any|dst-startip <IP> dst-end-ip <IP>] [all|dst-start-port <1-65535> dst-end-port <1-65535>] rule <1-20>	Permits protocols between 1 and 254.
	• [any|src-start-ip <IP> src-end-ip <IP>]- any is an abbreviation for a source IP of 0.0.0.0 and end IP 255.255.255.255
	  • src-start-ip <IP> - The keyword <src-start-ip> is the source IP address of the network. For example, 10.1.1.10/24 indicates the first 24 bits of the source IP is used for matching
	  • src-end-ip <IP> - The keyword <src-end-ip> is the source end IP address of the network
	• [any|dst-start-ip <IP> dst-end-ip <IP>] - any is an abbreviation for a destination start / end IP of the network.
	  • dst-start-ip <IP> - Defines the destination start IP address
	  • dst-end-ip <IP> - Defines the destination end IP address
	• [all|dst-start-port <1-65535> dst-end-port <1-65535>] - Permits all the packets
	  • dst-start-port <1-65535> - Defines the destination start port
	  • dst-end-port <1-65535> - Defines the destination end port
	• rule <1-20> - Define an integer value between 1 and 20. This value sets the rule precedence on the AAP

Example

```
RFSController(config-aap-ipfilter)#permit tcp src-start-ip 192.168.1.234
src-end-ip 192.168.1.9 dst-start-ip 10.0.0.0 dst-end-ip 10.0.0.255 all rule
rule 1
RFSController(config-aap-ipfilter)#
```

service

AAP IP Filter config commands

Invokes service commands used troubleshoot or debug `(config-if)` instance configurations

Supported in the following platforms:

- Mobility RFS4000 Controller
- Mobility RFS6000 Controller
- Mobility RFS7000 Controller

Syntax

```
service show cli
```

Parameters

None

Example

```
RFController(config-aap-ipfilter)#service show cli
AAP IPFilter Config mode:
+-clrscr [clrscr]
+-help [help]
+-show
  +-commands [show commands]
    +-WORD [show commands WORD]
  +-ip
    +-http
      +-secure-server [show ip http secure-server]
      +-server [show ip http server]
    +-access-group
      +-WORD [show ip access-group `WORD|ge <1-8> |me1|up1|wwan|vlan
<1-4094>']
        +-ge
          +-<1-8> [show ip access-group `WORD|ge <1-8> |me1|up1|wwan|vlan
<1-4094>']
        +-me1 [show ip access-group `WORD|ge <1-8> |me1|up1|wwan|vlan
<1-4094>']
        +-up1 [show ip access-group `WORD|ge <1-8> |me1|up1|wwan|vlan
<1-4094>']
        +-wwan [show ip access-group `WORD|ge <1-8> |me1|up1|wwan|vlan
<1-4094>']
        +-vlan
          +-<1-4094> [show ip access-group `WORD|ge <1-8> |me1|up1|wwan|vlan
<1-4094>']
        +-all [show ip access-group all]
        +-role [show ip access-group role ( WORD | )]
          +-WORD [show ip access-group role ( WORD | )]
      +-access-list [show ip access-list]
      +-arp [show ip arp]
      +-ddns
        +-binding [show ip ddns binding]
      +-dhcp
        +-binding [show ip dhcp binding]
          +-manual [show ip dhcp binding manual]
        +-class [show ip dhcp class ( WORD | )]
          +-WORD [show ip dhcp class ( WORD | )]
```

```
        +-pool [show ip dhcp pool ( WORD | )]
          +-WORD [show ip dhcp pool ( WORD | )]
        +-sharednetwork [show ip dhcp sharednetwork]
      +-dhcp-vendor-options [show ip dhcp-vendor-options]
      +-domain-name [show ip domain-name]
      +-dos
        +-config [show ip dos config]
        +-stats [show ip dos stats]
      +-igmp
        +-snooping [show ip igmp snooping]
          +-mrouter
            +-vlan
              +-<1-4094> [show ip igmp snooping mrouter
vlan(<1-4094>|VLAN)].....................
RFController(config-aap-ipfilter)#
```

show

AAP IP Filter config commands

Displays current system information running on the controller

Supported in the following platforms:

- Mobility RFS4000 Controller
- Mobility RFS6000 Controller
- Mobility RFS7000 Controller

NOTE
The following commands display only for the Mobility RFS6000 Controller and the Mobility RFS4000 Controller
- power
The following commands display only for the Mobility RFS7000 Controller and the Mobility RFS4000 Controller:
- port-channel
- static-channel-group

NOTE
For more details on the show command see *show on page 59*

Syntax

```
show <paramater>
```

Parameters

?	Displays all the parameters for which information can be viewed using the show command

Example

```
RFController(cconfig-aap-ipfilter)#show ?
  access-list           Internet Protocol (IP)
  aclstats              Show ACL Statistics information
  alarm-log             Display all alarms currently in the system
  autoinstall           autoinstall configuration
  banner                Display Message of the Day Login banner
  boot                  Display boot configuration.
  clock                 Display system clock
  commands              Show command lists
  crypto                encryption module
  debugging             Debugging information outputs
  dhcp                  DHCP Server Configuration
  environment           show environmental information
  file                  Display filesystem information
  firewall              Wireless firewall
  ftp                   Display FTP Server configuration
  history               Display the session command history
  interfaces            Interface status
  ip                    Internet Protocol (IP)
  ldap                  LDAP server
  licenses              Show any installed licenses
  logging               Show logging configuration and buffer
```

```
  mac                   Internet Protocol (IP)
  mac-address-table     Display MAC address table
  mac-name              Displays the configured MAC Names
  management            Display L3 Managment Interface name
  mobility              Display Mobility parameters
  ntp                   Network time protocol
  password-encryption   password encryption
  port-channel          Portchannel commands
  port                  Physical/Aggregate port interface
  privilege             Show current privilege level
  protocol-list         List of protocols
  radius                RADIUS configuration commands
  redundancy            Display redundancy group parameters
  role                  Configures role parameters
  rtls                  Real Time Locating System commands
  running-config        Current Operating configuration
  securitymgr           Securitymgr parameters
  sessions              Display current active open connections
  smtp-notification     Display SNMP engine parameters
  snmp                  Display SNMP engine parameters
  snmp-server           Display SNMP engine parameters
  spanning-tree         Display spanning tree information
  startup-config        Contents of startup configuration
  static-channel-group  static channel group membership
  terminal              Display terminal configuration parameters
  timezone              Display timezone
  traffic-shape         Display traffic shaping
  upgrade-status        Display last image upgrade status
  users                 Display information about currently logged in users
  version               Display software & hardware version
  virtual-ip            IP redundancy feature
  wireless              Wireless configuration commands
  wlan-acl              wlan based acl
  wwan                  Wireless wan interfaces

RFController(config-aap-ipfilter)#show
```